Symantec™ Client VPN

User’s Guide

Supported Platforms:

Microsoft® Windows® 2000

Microsoft Windows XP

Microsoft Windows ME

Microsoft Windows 98

Symantec Client VPN User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.0

PN: 10097553
August 19, 2003

Copyright notice

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/techsupp/ent/enterprise.html, select licensing and Registration, then select the product and version that you wish to register.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/. When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1 Introducing Symantec Client VPN

Section 1 Using Symantec Client VPN

Chapter 2 Installing Symantec Client VPN

Chapter 3 Getting started

Chapter 4 Configuring security gateways

Chapter 5 Configuring and connecting security gateway groups

Chapter 6 Connecting to a security gateway

Chapter 7 Using port control for personal firewall protection

Chapter 8 Managing Symantec Client VPN

Section 2 Administering Symantec Client VPN

Chapter 9 Supporting Symantec Client VPN Users

Chapter 10 Creating installation packages

Appendix A Remote policies

Appendix B Using digital certificates

Appendix C Troubleshooting

Appendix D Licensing

Index

Chapter 1

Introducing Symantec Client VPN

Symantec Client VPN is a Microsoft Windows-based software program that lets a remote user with Internet access connect to and use the resources of a private network as if the remote workstation was physically located inside of the protected network.

Symantec Client VPN creates a secure, tunneled connection between your computer and a private network. It can connect to Symantec security gateways and third-party security gateways as follows:

- Symantec security gateways that are configured to allow Symantec Client VPN to download VPN policies

  Symantec security gateways include any system that is running Symantec Enterprise Firewall with VPN, whether it is on Windows or Solaris, or on a Symantec Gateway Security appliance.
- Security gateways that are not configured to allow Symantec Client VPN to download VPN policies

  This includes third-party security gateways that are IPsec-compliant.

This chapter includes the following topics:

- Who should read this manual
- How this manual is organized
- Where to get more information about Symantec Client VPN
- How Symantec Client VPN works
- Extended user authentication methods
- Connecting to the Internet

Who should read this manual

Section 1 of this manual is intended for the remote client user who will connect to a private network using Symantec Client VPN. A remote user may also be required to install the client software, and perform basic configuration tasks.

It is assumed that a remote user is experienced with a personal computer, is comfortable installing applications on Microsoft Windows 2000, XP, ME, or 98 systems, and understands the principles of remote access.

Section 2 of this manual is intended for administrators who support remote users. It is assumed that these administrators have a complete understanding of their corporate security gateway environment and access to all information necessary to support their users.

How this manual is organized

Because corporate strategies for remote connectivity vary, there are many scenarios for installing, configuring, and connecting with Symantec Client VPN.

For example, some information technology (IT) departments will completely set up Symantec Client VPN, including installation and the configuration of the necessary security gateways. You may only need to read Chapter 3, Getting started, and Chapter 6, Connecting to a security gateway, although you may find other chapters helpful in customizing your Symantec Client VPN environment.

Other IT departments will provide you with the information and files you need to install and configure Symantec Client VPN with the help of this book.

Table 1-1 provides a matrix to help you determine which chapters of this manual apply to you.

Table 1-1 Document structure

Title	Content	Recommended for
Chapter 1, Introducing Symantec Client VPN	This chapter, which describes the organization of this book, where to get additional information, and provides an overview of how Symantec Client VPN works.	All users.
Section 1 – Using Symantec Client VPN		All users
Chapter 2, Installing Symantec Client VPN	Describes how to install the Symantec Client VPN software, including: ■ Verifying system requirements ■ Gathering needed information ■ Installing Symantec Client VPN ■ How to upgrade previous installations ■ How to uninstall the client software	Users who must install the Symantec Client VPN software.
Chapter 3, Getting started	Describes basic tasks involved in logging on and using the Symantec Client VPN software.	All users.
Chapter 4, Configuring security gateways	Describes how to configure security gateways. Configuration instructions are provided for:	
	■ Configuring for connections to Symantec security gateways that support autodownload of VPN policies and tunnel information.	Users who will connect to Symantec security gateways that support autodownload of VPN policies and tunnel information.
	■ Configuring for connections to security gateways that do not support autodownload of VPN policies and tunnel information. Includes how to configure the tunnel information, and IKE and VPN policies required to make a connection.	Users who will connect to security gateways that do not support autodownload of VPN policies and tunnel information. Users will need to manually configure VPN policies and tunnel information.
Chapter 5, Configuring and connecting security gateway groups	Describes how to configure Symantec Client VPN to use a security gateway group to connect to a security gateway.	All users.
Chapter 6, Connecting to a security gateway	Describes how to make a connection to a security gateway, and how to configure connection options.	All users.

Table 1-1 Document structure (Continued)

Title	Content	Recommended for
Chapter7, Using port control for personal firewall protection	Describes how to use the Symantec Client VPN port control features to provide personal firewall protection or to enable file and print sharing with other users in an environment that is protected by a firewall.	All users.
Chapter 8, Managing Symantec Client VPN	Describes how to manage Symantec Client VPN connections, including: ■ Viewing and managing client log data, and system statistics ■ Updating software using Symantec's LiveUpdate server ■ Deleting logged on users	All users.
Section 2 – Administering Symantec Client VPN		VPN administrators
Chapter 9, Supporting Symantec Client VPN Users	Describes user installation options, how to create a preconfigured or silent installation, and how to help provide users with configuration information.	VPN administrators
Chapter 10, Creating installation packages	Describes how to use the Symantec Packager to create an installation package,	VPN administrators
Appendix A, Remote policies	Describes the use of remote policies to provide configuration information.	Users who have received remote policy files.
Appendix B, Using digital certificates	Describes how to configure, use, and restore an Entrust digital certificate.	Users who have received Entrust certificate profiles.
Appendix C, Troubleshooting	Describes how to access the Knowledge base information about Symantec Client VPN that is provided on the Symantec Web site.	All users.
Appendix D, Licensing	Describes Symantec Client VPN licensing	All users

Where to get more information about Symantec Client VPN

The following documents contain additional information about Symantec Client VPN:

- *Symantec™ Client VPN Quick Start Card*

  This card provides a high level description of how to log on, configure a security gateway, and connect to a security gateway.

- *Symantec™ Client VPN Release Notes*

For information on configuring your security gateway for connectivity to Symantec Client VPN, see your security gateway documentation.

For the latest information on Symantec network security products, visit our World Wide Web site at www.symantec.com.

Online documentation

An online version of the Symantec Client VPN documentation set (in PDF format) is located in the ClientVPN\AES_3DES_DES directory on the Symantec Client VPN product CD-ROM.

These same documents can also be accessed at any time from **Start** > **Programs** > **Symantec Client VPN** > **Documentation** after you install the Symantec Client VPN software on your computer.

You can read these documents using the Adobe Acrobat Reader.

To obtain the Acrobat Reader, you can install it from the Symantec product CD-ROM. You can also download it free of charge from the Symantec Corporation Web site at www.symantec.com or from the Adobe Web site at www.adobe.com.

How Symantec Client VPN works

Symantec Client VPN uses the Internet Key Exchange (IKE) and the Internet Protocol security (IPsec) tunneling protocols to establish and manage secure connections.

Symantec Client VPN does the following:

- Negotiates tunnel parameters.
- Establishes secure tunnels according to defined parameters.

- Authenticates users by confirming their identity using user names, passwords, and a shared secret or digital certificates.
- Establishes user access rights, including some or all of the following: hours of access, connection time, allowed destinations or protocols.
- Manages security keys for encryption and decryption.
- Authenticates, encrypts, and decrypts data through the secure tunnel.

Security gateways

Before you can connect, a security gateway must be configured on the Symantec Client VPN machine that corresponds to the security gateway to which you will connect.

There are two types of security gateway configurations:

- If you are connecting to a Symantec security gateway, typically you only need to provide the IP address and authentication method for your security gateway. When your connection is made, the VPN policy and tunnel information for your connection are automatically downloaded by Symantec Client VPN.
- If you are connecting to a security gateway that does not support autodownload of VPN policies and tunnel information, or if you choose not to autodownload tunnels, you must manually configure the VPN policy and tunnel information.

In addition, if you are connecting to a Symantec security gateway, your IT administrator can create a remote policy that contains preconfigured security gateways. After you install the remote policy, no further configuration is required. For more information, see “Remote policies” on page 141.

Secure tunnels

Using the Symantec Client VPN software, there are two ways you can establish secure tunnels:

- You can manually initiate a connection by using the Symantec Client VPN GUI.
- You can select to have a security gateway and its tunnels automatically connected each time you log on to Symantec Client VPN.

Secure tunnels remain connected until one of the following occurs:

- You manually disconnect the security gateway.
- A timeout occurs.
- An Internet connection is lost.
- You exit Symantec Client VPN.
- You shut down your machine.

Security protocols

To ensure the safe transmission of data between the VPN client and the security gateway, Symantec Client VPN uses the following standardized security protocols:

- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- IP security (IPsec)

Note: Access to Symantec Client VPN is password protected to prevent others from using the secure tunnels into the VPN server.

Extended user authentication methods

An extended authentication method works in addition to your Symantec Client VPN logon password and Phase 1 authentication.

Extended user authentication takes place between Phase 1 and Phase 2 IKE negotiations. After you type the required user name and any other required information for your authentication method (such as a password or PIN), phase 2 negotiations begin and secure tunnels are downloaded from the security gateway.

Your security gateway administrator must supply you with a user name and password for the extended authentication method used by your organization.

Strong extended user authentication methods

Strong extended user authentication methods use single-use passwords. Symantec Client VPN supports the following strong extended user authentication methods:

- Defender tokens
- S/Key
- SecurID (ACE/Server)

Other extended user authentication methods

Other extended user authentication methods that are not as strong as the previous ones include:

- Gateway password
- Lightweight Directory Access Protocol (LDAP)
- NT 4.0 Domain
- RADIUS

Note: Active Directory authentication is supported by way of LDAP and RADIUS. It is not supported when using NT 4.0 Domain authentication.

Connecting to the Internet

Symantec Client VPN supports the services described in Table 1-2 for connecting to the Internet.

Table 1-2 Internet connection methods

Service	Description
Plain Old Telephone Service (POTS)	Connection by means of an analog dial-up modem.
Integrated Services Digital Network (ISDN)	Connection by means of a digital dial-up modem.
Cable	Connection by means of a cable modem.
Digital Subscriber Line (DSL)	Connection by means of a DSL modem.
PPPoE[a]	Connection by means of Point-to-Point Protocol over Ethernet
PPPoA[a]	Connection by means of Point-to-Point Protocol over Asynchronous Transfer Mode (ATM)
T1	Connection by means of a T1 line.
Direct Ethernet connection	Connections that are made directly, using the Ethernet.

[a] For details on using these connection methods, see the Symantec Knowledge Base, as described in "Accessing troubleshooting information" on page 151.

For PPPoA, see also the *Symantec Client VPN Release Notes.*

Section 1

Using Symantec Client VPN

Use this section and the appendices if you are an end user of Symantec Client VPN.

It contains the following chapters:

If you are an administrator who supports users of Symantec Client VPN, see Section 2, “Administering Symantec Client VPN” on page 113.

Chapter 2

Installing Symantec Client VPN

Before you begin to install the Symantec Client VPN software, make sure you have fulfilled the preinstallation requirements and that you have all of the information you need to install and use the client software.

This chapter includes the following topics:

- Verifying system requirements
- Gathering required account information
- Installing Symantec Client VPN
- Upgrading RaptorMobile 6.5.x installations
- Uninstalling Symantec Client VPN

Verifying system requirements

Before you begin, verify that your computer meets the minimum system requirements.

Operating systems

Symantec Client VPN supports the following operating systems:

- Microsoft Windows 2000: Professional, Server, or Advanced Server, Service Pack 3 or higher
- Microsoft Windows XP: Home or Professional; with Service Pack 1 or higher
- Microsoft Windows Millennium Edition
- Microsoft Windows 98 (Second Edition)

Note: Installing Symantec Client VPN on Microsoft Windows 2000 or XP requires local administrative privileges. If you do not have administrator privileges, someone who has administrator privileges for your machine must perform the installation for you.

Symantec Client VPN does not support upgrading your Windows operating system while Symantec Client VPN is installed. If you want to upgrade your operating system, uninstall Symantec Client VPN, perform the upgrade, and then re-install Symantec Client VPN.

Hardware configuration

Symantec Client VPN requires the following minimum hardware configuration:

- Pentium II or higher
- 20 MB free hard drive space for files
- 128 RAM
- CD-ROM drive, if installing from a CD
- Microsoft TCP/IP must be installed and bound to the network adapters that will be used by the Symantec Client VPN.
- Network Interface Cards (NICs)

  Your NIC must be installed and configured as you intend to use it with Symantec Client VPN.

  Symantec Client VPN binds to all adapters.

Symantec Client VPN supports dial-up adapters and NICs tested and qualified for use by Microsoft. The following interface configurations are supported:

- Dial-up
- One or more NICs (Ethernet)
- Selected cards that implement the IEEE 802.11B wireless LAN standard
- Dial-up and one or more NICs (Ethernet)

The following NICs have known limitations and are not supported:

- Linksys EC2T PCMCIA Ethernet card
- HP EN-1207D-TX PCI 10/100 Fast Ethernet Model
- D-Link Access Point DWL-650 wireless card

  Note: When tested in Microsoft Windows 2000, the D-Link Access Point DWL-650 wireless card worked in a Dell Latitude LS laptop computer, model PP01S only.
- Orinoco Silver 64-bit and Gold 128-bit Encryption, 5-volt wireless cards (Windows 98 and Windows ME only)

Testing Microsoft TCP/IP installation

You can verify that Microsoft TCP/IP is installed and properly bound if your administrator has enabled pings.

Note: By default, pings are disabled on the security gateway. In this case, ping another system on your local network.

To test TCP/IP

1. Connect to the Internet.
2. Click **Start** > **Run**.
3. Type the following command:

   ping <IP address>

   where <IP address> is the IP address or fully qualified domain name of the security gateway.

   If a DOS box display showing a reply, TCP/IP is properly installed. If the request times out, contact your IT administrator to determine what the problem is.

Network requirements

Verify that you have one of the following network connections:

- A direct network connection (T1, cable, wireless, or DSL modem and Network Interface Card (NIC), as described in “Hardware configuration” on page 22).
- An Internet connection (internal/external analog or digital modem).

  This also assumes that you have a valid account with an Internet Service Provider (ISP) and that the ISP client or dialer information has been properly configured on your workstation.

Additional preinstallation considerations

In addition to the hardware and software requirements, ensure that your system meets the following preinstallation requirements:

- Remove conflicting VPN client software

  Symantec Client VPN cannot install with any other VPN client. If another VPN client such as Microsoft’s VPN Client is running on your system you must uninstall it.

  If you do not uninstall the following VPN clients, the installation program will detect them, display an error message, and terminate:

  - Nortel VPN Client
  - Check Point SecuRemote
  - Cisco VPN Client

- Configure router IP addresses and subnets for use with Symantec Client VPN

  If you connect to Symantec Client VPN through a home router using Network Address Translation (NAT), you may have a non-unique IP address that may conflict with another connected user.

  Before you install, you should modify the default subnet assigned by your router. In consultation with your security gateway administrator, choose a subnet that will not be used by another VPN user in your environment.

- If you will install Symantec Client VPN on an NTFS partition, grant write to the ClientVPN directory for all users who will use the client.

Gathering required account information

Verify with your security gateway administrator or IT department that an account has been established for you, and obtain the following information:

- The IP address or fully qualified domain name of the security gateway to which you are connecting.
- Your Client Phase 1 ID (user name).
- Your Gateway Phase 1 ID (if applicable and if it differs from the security gateway's IP address).
- One of the following:
    - If you will authenticate using a shared secret, the shared secret defined on the security gateway.
    - If you will authenticate using a digital certificate, obtain a profile with the certificate (for example, user.epf) along with a password.
- If your network uses a form of extended authentication (for example, a Defender Server or a SecurID ACE/Server), verify that you have all of the necessary tokens, user names, and passwords for the specified method.
- Check with your security gateway administrator or IT department to see if a Remote Policy file has been created to perform initial client configuration tasks. If it has, make sure that you receive the file and, optionally, a Remote Policy install password.

  See "Remote policies" on page 141.
- If you use a dial-up connection, make sure that you have the logon credentials for your Internet Service Provider (ISP). This is usually a user name and password.

In addition, if the security gateway to which you will connect does not support autodownload of VPN policies and tunnel information, you will also need the following:

- IKE policy details for each security gateway
- IP address and subnet mask for each secure tunnel
- VPN policy details for each secure tunnel

Installing Symantec Client VPN

Your installation options depend on the approach chosen by your security gateway administrator or IT department.

- Your administrator may choose to install and configure the client software on your workstation; you may only need to log on and authenticate with the security gateway.

  If the Symantec Client VPN software has already been installed for you, proceed to Chapter 3, Getting started, to start using the client software.

- You may install the client software yourself. In this case, your administrator will do one of the following:

  - Supply a CD-ROM, which automatically displays the client installation program when placed in the CD-ROM drive.
  - Instruct you to download the Symantec Client VPN software from a file share that has been set up for your use.

    Unzip the file and copy the resulting folder to the top level of one of your hard drive partitions.

  If you are installing the client software, complete the installation procedures contained in the rest of this chapter.

Before you begin

Before installing Symantec Client VPN, complete the following tasks, if applicable:

- Close all other applications.

  You may encounter errors if you attempt to install or uninstall Symantec Client VPN while your dial-up application is running.

- If you have any version of RaptorMobile running on the client workstation, uninstall it before installing Symantec Client VPN.

  See “Upgrading RaptorMobile 6.5.x installations” on page 29.

- If Symantec Enterprise VPN Client version 7.0 or later is installed, you can upgrade without uninstalling.

- If you have received a remote policy from your administrator and you are installing from downloaded software, copy the remote policy to the location of the setup.exe file before installing.

  See “Installing remote policy files” on page 143.

Installing Symantec Client VPN, or upgrading from Symantec Enterprise VPN Client version 7.0

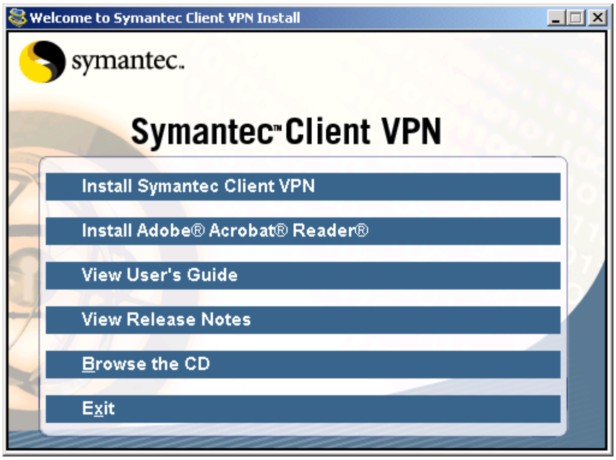
Follow the instructions in this section to install Symantec Client VPN.

If you have already installed Symantec Enterprise VPN Client version 7.0 or later, you should not remove it. Simply install the new software to upgrade.

When you upgrade, your Symantec Enterprise VPN Client version 7.0 configuration files are copied to the new location of the Symantec Client VPN version 8.0 software. The 7.0 VPNClient directory is replaced by the 8.0 ClientVPN directory.

To install Symantec Client VPN

1. Depending on how you received the Symantec Client VPN software, do one of the following:
   - If you received the *Symantec Client VPN* CD, place it in your CD-ROM drive.

     
     Welcome to Symantec Client VPN Install
symantec.
Symantec™ Client VPN
Install Symantec Client VPN
Install Adobe® Acrobat® Reader®
View User's Guide
View Release Notes
Browse the CD
Exit

     In the Welcome to Symantec Client VPN Install dialog box, click **Install Symantec Client VPN**.
   - If you downloaded the installation files, navigate to the location of the setup.exe file and double-click **setup.exe**.
2. A screen message prompts you to close all applications before continuing. Verify that all applications are closed, and then click **OK**.

3. In the Welcome to the InstallShield Wizard for Symantec Client VPN dialog box, click **Next**.

   Note: If you have a previous version of Symantec Client VPN installed, the Welcome dialog box notifies you that the previous software has been detected and will be upgraded.

4. Review the terms of the License Agreement, and do one of the following:
   - To accept the license agreement, click **Yes**.
   - To exit the installation program, click **No**.
5. In the View Release Notes dialog box, do one of the following:
   - To display the release notes immediately, click **Next**.

     The release notes are displayed in a browser window. When you are finished reading them, close the window to return to the installation procedure.
   - To continue without reading the release notes, select **View the release notes later**, and then click **Next**.
6. In the Choose Destination Location dialog box, do one of the following:
   - To accept the default destination for the Symantec Client VPN files, click **Next**.
   - To select a different location to install the files, click **Browse**.

     In the Choose Folder window, specify a new path by typing the path or choosing a directory, click **OK**, and then click **Next.**
7. In the Symantec Client VPN Installation Options dialog box, select whether you want to add a folder to your Start menu and whether you want to add a Symantec Client VPN shortcut icon to your desktop.

   If you select Create a Start Menu folder, the folder Symantec Client VPN is added to the Program folder. The options in this folder let you start or uninstall Symantec Client VPN, and provide easy access to the product documentation and Help.
8. Click **Next**.

9 In the Installation Review dialog box, review the selections you have made and do one of the following:

- To display previous dialog boxes so that you can change your installation choices, click **Back**.
- To start the installation, click **Next**.

Note: If you are upgrading from Symantec Enterprise VPN Client version 7.0 or later, the Installation Review dialog box gives you the location to which your saved configuration files will be copied and notifies you that your old directory will be deleted.

10 In the Setup Complete dialog box, select whether you want to restart your computer now or later, and then click **Finish**.

Note: You must restart your computer before you can use the Symantec Client VPN software.

After you complete the installation, you should run LiveUpdate to assure that the latest revision of Symantec Client VPN is installed. See "Updating software using LiveUpdate" on page 109.

Installing and using the Adobe Acrobat Reader

The Symantec Client VPN online documentation is provided in PDF format. To view PDF files, you must have access to the Adobe Acrobat Reader.

If Adobe Acrobat Reader is not already installed on your system, you can install it from the Welcome to Symantec Client VPN Install screen that displays when you install from the *Symantec Client VPN* CD, or you can download the files from the Adobe Web site at http://www.adobe.com.

Upgrading RaptorMobile 6.5.x installations

This section describes how to upgrade if your previous Symantec mobile client was RaptorMobile 6.5.X.

To upgrade from RaptorMobile version 6.5.X

If you have RaptorMobile version 6.5.X installed, you must:

- Uninstall RaptorMobile.
- Install Symantec Client VPN version 8.0.

To uninstall RaptorMobile

1 On the taskbar, click **Start** > **Programs** > **Axent** > **RaptorMobile** > **Uninstall.**

2 When asked if you are sure you want to remove RaptorMobile and all of its components, click **Yes.**

3 When you are warned to close open applications, make sure all applications are closed, and then click **OK.**

   The Remove Programs from Your Computer dialog box shows the progress of the uninstall.

4 When asked if you want to destroy your secure tunnel configuration files, do one of the following:

   - To save the configuration information for secure tunnels, port control and preferences, click **No.**

     Your tunnel information will be saved in the following file:

     C:\Program Files\Axent\RaptorMobile\USERS\<user>.dat

     where <user> is your user name.

     After you install Symantec Client VPN software, this tunnel information is available to you when you run Symantec Client VPN.

   - To remove all tunnel information, click **Yes.**

     All files are removed from your system.

   Screen messages show that the VPN driver and Symantec Client VPN software is being uninstalled from your system.

5 When asked to reboot, do one of the following:

   - To reboot now, click **Yes.**
   - To reboot at a later time, click **No.**

6 Click **OK.**

Note: You must reboot to complete the uninstall of RaptorMobile, and before you can install Symantec Client VPN.

To install Symantec Client VPN version 8.0

◆ Complete the installation procedure described in "Installing Symantec Client VPN, or upgrading from Symantec Enterprise VPN Client version 7.0" on page 27.

Uninstalling Symantec Client VPN

You can uninstall the Symantec Client VPN software from the Uninstall option of the Symantec Client VPN program group. You can also uninstall Symantec Client VPN by using the Add/Remove programs feature of Microsoft Windows.

To uninstall Symantec Client VPN

1. On the taskbar, click **Start** > **Programs** > **Symantec Client VPN** > **Uninstall**.
2. When asked if you are sure you want to remove Symantec Client VPN from your computer, click **Yes**.
3. When asked if you want to destroy your secure tunnel configuration files, do one of the following:
   - To save the configuration information for secure tunnels, port control and preferences, click **No**.

     Your tunnel information is saved in the following file:

     C:\Program Files\Symantec\ClientVPN\USERS\<user>.dat

     where <user> is your user name.

     If you reinstall the Symantec Client VPN software, this tunnel information is available to you when you run Symantec Client VPN.
   - To remove all tunnel information, click **Yes**.

     All files are removed from your system.

   Screen messages show that the VPN driver and Symantec Client VPN software is being uninstalled from your system.
4. In the Uninstall Complete dialog box, select whether to restart your computer now or later.

   Note: The uninstall is not complete until you restart your system.
5. Click **Finish**.

Chapter 3

Getting started

This chapter describes how to start using Symantec Client VPN.

It includes the following topics:

- Logging on to Symantec Client VPN
- Symantec Client VPN user interface
- Configuring logon options
- Verifying the Symantec Client VPN version
- Logging off from Symantec Client VPN

Logging on to Symantec Client VPN

Before you log on, make sure that your security gateway administrator and internet service provider have given you all user names, passwords, and any additional information required to connect to your security gateway.

See "Gathering required account information" on page 25.

If a local user name and password have not been preconfigured, you choose a user name and password to create the local profile. This local profile user name and password is used to identify you when you log on to Symantec Client VPN. The account does not necessarily have to match any existing user name and password credentials that you have received for use in establishing connections.

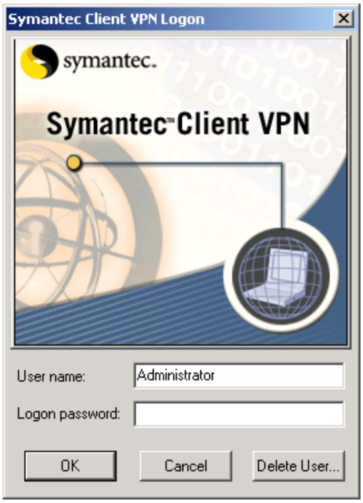
Symantec Client VPN saves this local information and any other changes you make as your personal Symantec Client VPN user profile.

To log on to Symantec Client VPN

1 If you plan to connect to a security gateway, establish your Internet connection.

2 Do one of the following:

- On the desktop, double-click Symantec Client VPN.
- In the system tray on the right side of the Windows task bar, right-click the Symantec Client VPN icon and select **Open Symantec Client VPN**.
- Select **Start** > **Program Files** > **Symantec Client VPN** > **Symantec Client VPN**.



User name: Administrator

Logon password:

3. In the Symantec Client VPN Logon dialog box, in the User name text box, type your user name.

   By default, the User name text box contains the name you used to log on to your Microsoft Windows workstation.

4. In the Logon password text box, type your password.

   Passwords are case-sensitive, and, for security purposes, are not displayed on the screen.

5. Click **OK**.

6. If you are logging on for the first time, do the following:

   - In the New user password dialog box, in the Verify password text box, retype your password.

     Click **OK**.

   - If there is a remote policy file in the ClientVPN directory, you are asked if you want to install it.

     To install it, click **Yes**, and, if prompted, type the remote policy install password that your system administrator has provided.

     See “Remote policies” on page 141.

   The Symantec Client VPN user interface displays on your desktop.

After your initial log on, you can set logon options to change the behavior of this basic logon procedure, as described in “Configuring logon options” on page 42.

Symantec Client VPN user interface

The Symantec Client VPN dialog box appears after you have successfully logged on to the client software. This window lets you access all dialogs and controls to configure client operations.

Figure 3-1 Symantec Client VPN dialog box

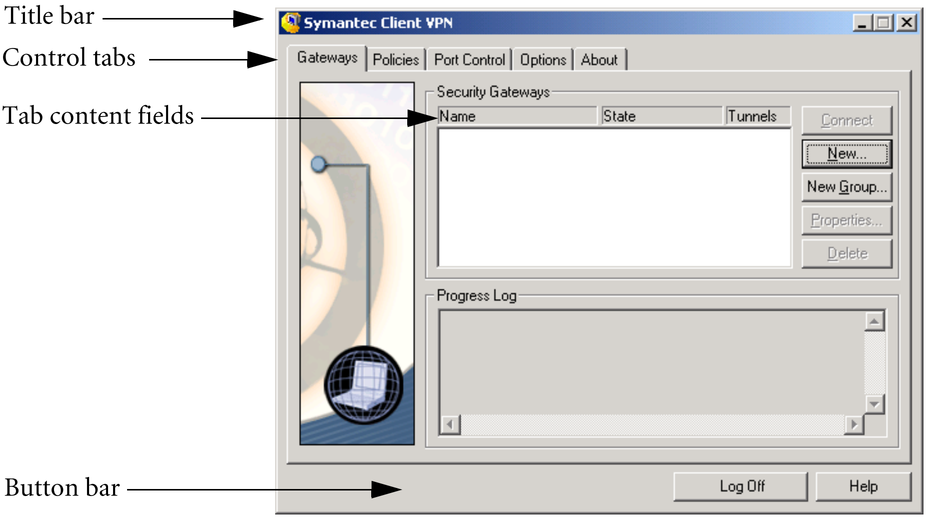


Table 3-1 describes the Symantec Client VPN user interface controls.

Table 3-1 Symantec Client VPN user interface controls

Control	Description
Title bar	Displays the application's title. The title bar also contains the minimize (-) and exit (x) buttons. ■ Click minimize to shrink the application to an icon in the Windows system tray. The application is still active, and, if you are connected, the connection remains open. ■ Click exit to disconnect all secure tunnels and shut down the Symantec Client VPN application.
Control tabs	Consists of five tabs (Gateways, Policies, Port Control, Options, and About) that let you access all client features and functions.
Tab content fields	Displays the contents of each tab. The content changes as you select each tab. Within each content field, additional buttons and controls let you configure Symantec Client VPN features.

Table 3-1 Symantec Client VPN user interface controls (Continued)

Control	Description
Button bar	Contains the Log Off and Help buttons. ■ Click Log Off to exit the application. ■ Click Help on any window or dialog box to launch the Symantec Client VPN Help system.

Using the Symantec Client VPN control tabs

Table 3-2 describes the control tabs of the Symantec Client VPN GUI and the functions you can access from them:

Table 3-2 Symantec Client VPN tabs

Tab	Description
Gateways	Use this tab to: ■ View the address, state, and associated secure tunnels for each security gateway. ■ Connect or disconnect a security gateway, or security gateway group. ■ Add or delete a security gateway, or security gateway group. ■ View the properties of an existing security gateway and its associated secure tunnels. ■ Add a secure tunnel.
Policies	Use this tab to view, define, edit, or delete the IKE and VPN policies.
Port Control	Use this tab to: ■ Specify the port control type. ■ Add or delete individual ports and protocols to solve connectivity problems. ■ Enable the ports required for file and print sharing.

Table 3-2 Symantec Client VPN tabs (Continued)

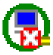
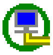
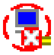
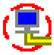
Tab	Description
Options	Use this tab to: ■ Set your user options. ■ View the log and system data. ■ Delete a user. ■ Change your Symantec Client VPN logon password. ■ Configure a digital certificate. ■ Run LiveUpdate. When you change a parameter in the Options tabs, you are prompted with a confirmation message before you can select another tab.
About	Use this tab to view the version and copyright information for Symantec Client VPN.

Using the system tray context menu

After you install Symantec Client VPN, an icon for the application appears in the system tray area in the lower right corner of the Windows task bar.

Table 3-3 shows how the Windows system tray icon changes to reflect the connection state and port control state of Symantec Client VPN:

Table 3-3 Windows system tray icon

Icon	Description
	Disconnected, protected (the port control type is set to Restricted or Restricted & Recent Calls, and file and print sharing is disabled)
	Connected, protected
	Disconnected, unprotected (the port control type is set to Wide Open or file and print sharing is enabled)
	Connected, unprotected

You can display a context menu for Symantec Client VPN by right-clicking on the Symantec Client VPN icon in the Windows system tray.

Table 3-4 provides a detailed description for each of the context menu options.

Table 3-4 Context menu options

Option	Description
Open Symantec Client VPN	Displays the Symantec Client VPN application on the desktop.
Connect (or Disconnect) <security gateway> or <security gateway group>	Lets you connect or disconnect from security gateways and security gateway groups that are configured in Symantec Client VPN. This control is a toggle: when a security gateway is connected, the disconnect option is available; when it is disconnected, the connect option is available. See "Viewing secure tunnel properties and status" on page 73. See "Connecting using a security gateway group" on page 84.
Display Log	Launches the Symantec Client VPN Log Viewer. The log window displays a detailed description of the current session's activity, including all notification and process information. See "Viewing log data" on page 106.
Port Control Settings	Opens the Symantec Client VPN application with the Port Control Settings tab displayed, so that you can change port settings. See "Using port control for personal firewall protection" on page 97.
Enable (or Disable) File and Print Sharing	This control is a toggle that lets you enable or disable file and print sharing. The Symantec Client VPN icon in the Windows system tray changes color and shape to indicate whether file and print sharing is enabled. See "Enabling and disabling file and print sharing" on page 103.

Table 3-4 Context menu options (Continued)

Option	Description
LiveUpdate	Launches the Symantec LiveUpdate application. LiveUpdate connects to the Symantec LiveUpdate server to check for program and other updates such as virus definitions and URL lists. When updates are available, you can instruct LiveUpdate to download them to your computer and install them, ensuring that all Symantec products on your computer are up-to-date, including your Symantec Client VPN software. See "Updating software using LiveUpdate" on page 109.
Exit	Causes all connections to close and the Symantec Client VPN application to terminate. Selecting Exit has the same effect as clicking Log Off or the close button (x) on the Symantec Client VPN GUI.

Using Symantec Client VPN Help

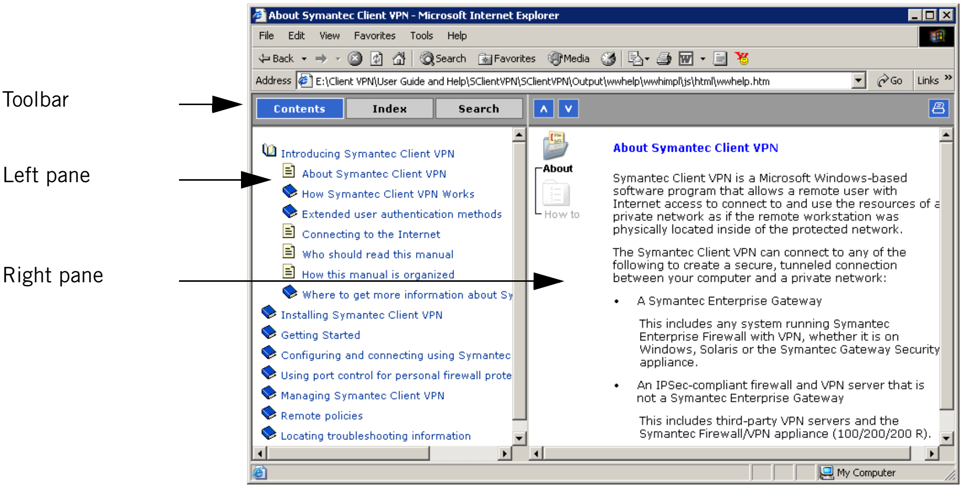
The Symantec Client VPN Help provides easy access to the content of the *Symantec Client VPN User's Guide* from any point in the Symantec Client VPN user interface.

For complex configurations, Help provides an additional level of detail. For example, when you create a VPN policy, Help describes the security options.

Help displays in a three-paned browser window:

- A toolbar across the top displays buttons that you can use to move around in the Help system.
- The left pane is a navigation frame that displays the Contents, Index, and Search tabs.
- The right pane displays the Help topics.

Figure 3-2 Symantec Client VPN Help window


Toolbar
Left pane
Right pane
About Symantec Client VPN - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address E:\Client VPN\User Guide and Help\SClientVPN\SClientVPN\Output\wwhelp\wwhimpl\js\html\wwhelp.htm
Go Links
Contents
Index
Search
About
How to
My Computer

Introducing Symantec Client VPN
About Symantec Client VPN
How Symantec Client VPN Works
Extended user authentication methods
Connecting to the Internet
Who should read this manual
How this manual is organized
Where to get more information about Sy
Installing Symantec Client VPN
Getting Started
Configuring and connecting using Symantec
Using port control for personal firewall prote
Managing Symantec Client VPN
Remote policies
Locating troubleshooting information

About Symantec Client VPN

Symantec Client VPN is a Microsoft Windows-based software program that allows a remote user with Internet access to connect to and use the resources of a private network as if the remote workstation was physically located inside of the protected network.

The Symantec Client VPN can connect to any of the following to create a secure, tunneled connection between your computer and a private network:

- A Symantec Enterprise Gateway

  This includes any system running Symantec Enterprise Firewall with VPN, whether it is on Windows, Solaris or the Symantec Gateway Security appliance.

- An IPSec-compliant firewall and VPN server that is not a Symantec Enterprise Gateway

  This includes third-party VPN servers and the Symantec Firewall/VPN appliance (100/200/200 R).

To display the Symantec Client VPN Help

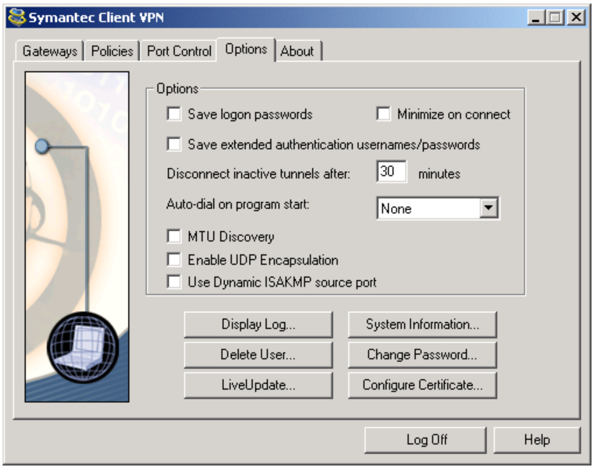
1. Do one of the following:
   - On any tab of the Symantec Client VPN dialog box, or on any dialog box that you display, click **Help**.
   - At any point in the Symantec Client VPN user interface, click **F1**.

   The Help that displays describes the dialog box in which you are working.
2. Use the Contents, Index, and Search tabs to access other Help topics.

Configuring logon options

After your initial log on, you can use the Options tab to configure Symantec Client VPN for a number of logon variations.

Figure 3-3 Symantec Client VPN Options tab



Options

☐ Save logon passwords ☐ Minimize on connect

☐ Save extended authentication usernames/passwords

Disconnect inactive tunnels after: 30 minutes

Auto-dial on program start: None

☐ MTU Discovery

☐ Enable UDP Encapsulation

☐ Use Dynamic ISAKMP source port

Your options include:

- Enabling and using Auto Dialer for a dial-up connection.

  This lets you establish your Internet connection as part of your logon procedure.

- Saving logon and certificate passwords.

- Changing your logon password.

- Configuring a digital certificate.

  This lets you use an Entrust certificate to authenticate to your security gateway when you log on. See “Using digital certificates” on page 147.

Enabling and using Auto Dialer for a dial-up connection

Symantec Client VPN includes an Auto Dialer feature that lets you select an Internet Service Provider (ISP) to which you automatically connect when you log on to Symantec Client VPN.

To enable and use Auto Dialer

You enable the Auto Dialer from the Options tab, by selecting an ISP that you have defined in Microsoft Windows.

Thereafter, when you log on, the software displays the Auto Dialer dialog box and prompts you to confirm your user name, password, and the phone number of the ISP you have selected to use.

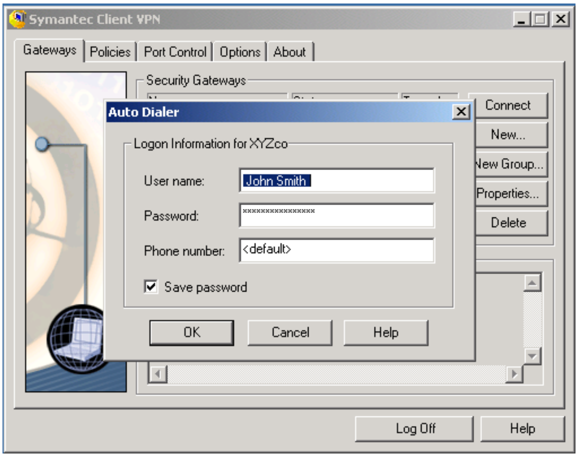
To select an ISP for a dial-up connection

1. Use your operating system's network and dial-up connection features to define the ISP on your system.
2. Log on to Symantec Client VPN.
3. On the Options tab, from the Auto-dial on program start drop-down list, select the name of the ISP to which you want Symantec Client VPN to connect.
4. When you change tabs or log off, you are asked if you want to apply your preference changes. Do one of the following:
   - To apply any changes, click **Yes**.
   - To clear any changes, click **No**.

To use the Auto Dialer when you log on

1. Launch Symantec Client VPN from the Windows desktop, Programs list, or system tray as described in "Logging on to Symantec Client VPN" on page 34.
2. In the Symantec Client VPN Logon dialog box, do the following:
   - In the User name text box, type your user name.
   - In the Logon password text box, type your password.

3 Click **OK**.



Logon Information for XYZco

User name: John Smith

Password: ****************

Phone number: <default>

☑ Save password

4 In the Auto Dialer dialog box, confirm your ISP user name and phone number.

You can change the ISP information at this time; however, the changes that you make are valid for the current log on attempt only.

To permanently change ISP information, you must reconfigure the ISP on your workstation and select it using Symantec Client VPN.

5 If required, type your password.

You do not have to type your password if Save Password is checked; however, the use of Save Password is less secure than entering a password each time you establish your Internet connection.

6 Click **OK**.

A message box shows the progress of your connection; you will see one of the following:

- If the connection is successful, the message box closes, leaving Symantec Client VPN open on your desktop.
- If the connection fails, click **Cancel** to close the message box.

  Verify that the information in the Auto Dialer dialog box is correct, and try again.

  If you are still unsuccessful, check the ISP configuration on your workstation. Also, contact the ISP to verify that your account is active and to confirm the accuracy of your log on credentials.

  You can still configure Symantec Client VPN, but you cannot connect to a security gateway without an Internet connection.

Changing your logon password

Complete the procedure described in this section to change your logon password.

To change your logon password

1. In Symantec Client VPN, on the Options tab, click **Change Password**.
2. In the Change Symantec Client VPN Password dialog box, in the Old password text box, type your current log on password.
   Passwords are case-sensitive.
3. In the New password text box, type a new password.
4. In the Verify password text box, retype your new password.
5. Click **OK**.

Saving logon and certificate passwords

To speed up the process of logging on, you can save your logon password, and, if you use a certificate, your certificate password.

Caution: Saving passwords reduces the security of your system because anyone with access to your computer can log on as you and connect to your internal network.

To save logon and certificate passwords

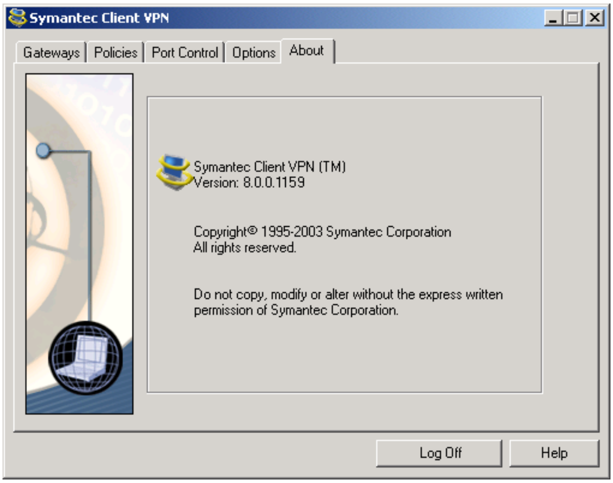
1. In Symantec Client VPN, on the Options tab, under Options, check **Save logon passwords**.
2. When you are warned that saving passwords can reduce the security of your system, do one of the following:
   - To save your passwords, click **Yes**.
   - To clear the Save logon passwords check box, click **No**.
3. When you change tabs or log off, you are asked if you want to apply your preference changes. Do one of the following:
   - To apply any changes, click **Yes**.
   - To clear any changes, click **No**.

Verifying the Symantec Client VPN version

You can verify the version number of and view copyright information for your Symantec Client VPN software.

To verify the Symantec Client VPN version

◆ In the Symantec Client VPN dialog box, click the **About** tab.



Symantec Client VPN (TM)
Version: 8.0.0.1159

Copyright© 1995-2003 Symantec Corporation
All rights reserved.

Do not copy, modify or alter without the express written permission of Symantec Corporation.

The final digits of the version number represent the build number. If you contact Symantec support, you should ascertain this number before you call.

Logging off from Symantec Client VPN

You have multiple options for logging off from Symantec Client VPN.

To log off from Symantec Client VPN

1 Do one of the following:

- In the Symantec Client VPN dialog box, click **Log Off**.
- In the Symantec Client VPN dialog box, in the right corner of the title bar, click **X**.
- In the Windows system tray, right-click the Symantec Client VPN icon, then, on the context menu, click **Log Off**.

2 If you have made any preference changes using the Options tab, you are asked if you want to apply them.

Do one of the following:

- To log off and apply any changes you have made, click **Yes**.
- To log off clear any changes you have made, click **No**.

3 If you are connected to any security gateways, a messages asks if you want to disconnect them. Do one of the following:

- To log off and disconnect from security gateways, click **Yes**.
- To leave your security gateways connected, click **No**. Log off at a later time.

Chapter 4

Configuring security gateways

Security gateways must be defined on Symantec Client VPN to establish a VPN tunnel.

Your security gateway administrator may configure security gateways for you, or provide preconfigured security gateways through a remote policy. These remote policies are available when you first log on to Symantec Client VPN. While you can define additional security gateways, you can use the security gateways defined in your remote policies immediately. See "Remote policies" on page 141.

To add additional security gateways, or if no security gateways exist, you can configure them yourself using the Gateways tab.

You can configure for two types of connections:

- One that supports autodownload of VPN policies and tunnel information to the client if you are connecting to Symantec security gateways.

  Symantec security gateways include Symantec Enterprise Firewall with VPN running on Windows or Solaris, and the Symantec Gateway Security appliances.

- One that does not support autodownload of VPN policies and tunnel information from the security gateway to which you will connect.

  You must use this method if you connect to third-party security gateways that are IPsec-compliant. You can choose to use it for connections to Symantec security gateways.

You can configure individual security gateways, as described in this chapter, or you can configure security gateway groups consisting of multiple security gateways. When you create a security gateway group and use it to connect, each security gateway in the group is tried until you get a successful connection. Security gateway groups are described in "Configuring and connecting security gateway groups" on page 79.

This chapter includes the following topics:

Configuring for connections that support autodownload of VPN policies and tunnel information

This section describes the simplest way to configure a security gateway.

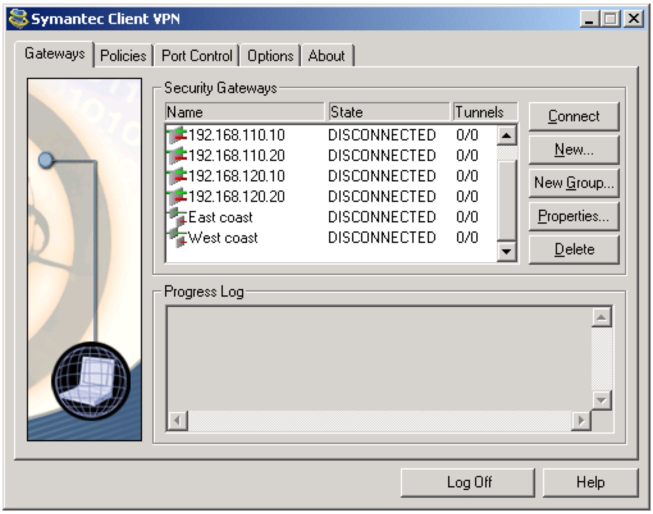
You can use this procedure when you will connect to a Symantec security gateway and want to download the tunnel information required for connection.

If you do not want to download tunnel information, see "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

To configure a new security gateway

1 Log on to Symantec Client VPN.

The Gateways tab shows the security gateways and security gateway groups that you have already defined.



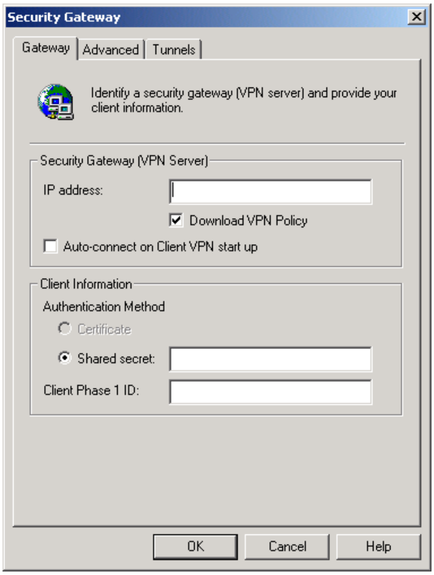
Name	State	Tunnels
192.168.110.10	DISCONNECTED	0/0
192.168.110.20	DISCONNECTED	0/0
192.168.120.10	DISCONNECTED	0/0
192.168.120.20	DISCONNECTED	0/0
East coast	DISCONNECTED	0/0
West coast	DISCONNECTED	0/0

Icons beside each entry indicate the type of security gateway:

Individual security gateway

Security gateway group

2 Click **New**.



Security Gateway

Identify a security gateway (VPN server) and provide your client information.

Security Gateway (VPN Server)

IP address:

☑ Download VPN Policy

☐ Auto-connect on Client VPN start up

Client Information

Authentication Method

○ Certificate

● Shared secret:

Client Phase 1 ID:

3 In the Security Gateway dialog box, on the Gateway tab, in the IP address text box, type the IP address or fully qualified domain name of the security gateway.

Use either a true dotted decimal IP address or a resolvable DNS name. This address is supplied by the security gateway administrator.

4 Verify that **Download VPN Policy** is checked.

This option is selected by default.

If you do not want your VPN policy and tunnel information automatically downloaded, uncheck this check box, and follow the procedure for "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

5 If you want this security gateway to automatically connect each time you start Symantec Client VPN, check **Auto-connect on Client VPN start up**.

6 Under Client Information, select one of the following authentication methods:

- Certificate

  To use Certificate authentication, you must copy an Entrust X.509 digital certificate to the \ClientVPN directory, and you must configure Symantec Client VPN to use the certificate before you can use it to make a connection. See "Using digital certificates" on page 147.

- Shared secret

  If you select Shared secret, in the text box beside the option button, type the shared secret key that is provided by your administrator.

  Note that if a shared secret begins with the value “0x”, it is interpreted to be a hexidecimal string. It must contain an even number of characters, and must be between 42 and 128 characters long.

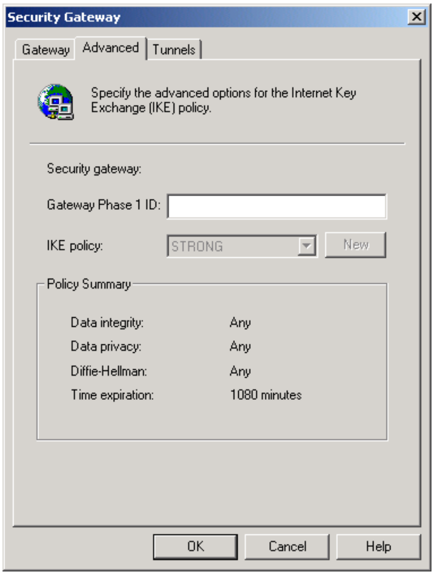
7 In the Client Phase 1 ID text box, type the Client Phase 1 ID that is provided by your administrator.

This may be your user name as it is configured by your administrator, or your user name for extended authentication.

8 If you have been given a Gateway Phase 1 ID, on the Advanced tab, in the Gateway Phase 1 ID text box, type the value.

The Gateway Phase 1 ID, also known as the Remote Phase 1 ID, should be the same as the security gateway Phase 1 ID. It is the identifier that allows phase 1 negotiations to proceed.

If you do not type a string here, by default the IP address of the security gateway is used as the Gateway Phase 1 ID.



Specify the advanced options for the Internet Key Exchange (IKE) policy.

Security gateway:

Gateway Phase 1 ID:

IKE policy: STRONG

Policy Summary

Data integrity:	Any
Data privacy:	Any
Diffie-Hellman:	Any
Time expiration:	1080 minutes

9 Click **OK**.

Configuring for connections that do not support autodownload of VPN policies and tunnel information

If the security gateway to which you will connect does not support autodownload of VPN policies and tunnel information, your administrator will give you this information.

This section describes how to configure a security gateway to make this type of connection. You can use it to configure for connections to third-party security gateways that are IPsec-compliant, or if you do not want to have VPN policy, IKE policy, and tunnel information automatically downloaded

If you have not been given this information, see "Configuring for connections that support autodownload of VPN policies and tunnel information" on page 50.

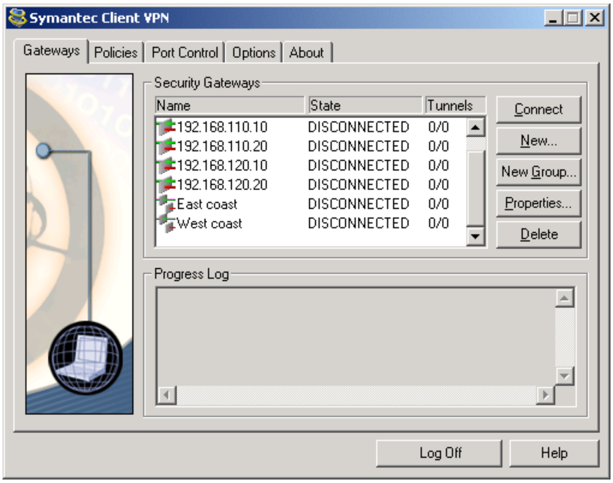
When connecting to a security gateway that does not support the automatic downloading of VPN policies and tunnel information by Symantec Client VPN, you must configure the following:

- Basic connection information, including the IP address of the security gateway, your Client Phase 1 ID, and either a shared secret or certificate configuration.
- The IKE policy used for phase 1 negotiation.
  See "Defining an IKE policy" on page 60.
- One or more secure tunnels.
  See "Adding a secure tunnel" on page 63.
- The VPN policies used in the secure tunnels.
  See "Defining a VPN policy" on page 66.

To configure the security gateway

1 Log on to Symantec Client VPN.

The Gateways tab shows the security gateways and security gateway groups that you have already defined.



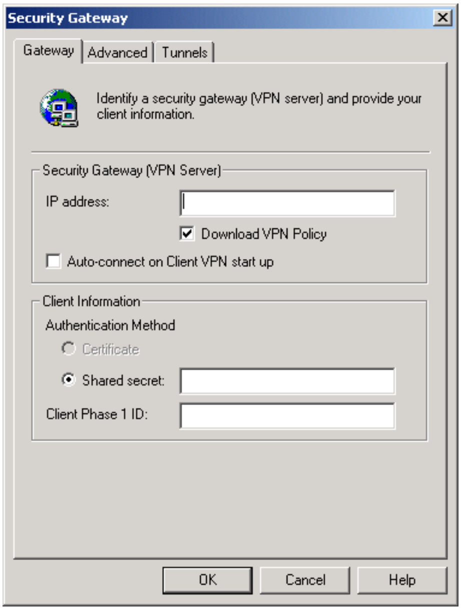
Name	State	Tunnels
192.168.110.10	DISCONNECTED	0/0
192.168.110.20	DISCONNECTED	0/0
192.168.120.10	DISCONNECTED	0/0
192.168.120.20	DISCONNECTED	0/0
East coast	DISCONNECTED	0/0
West coast	DISCONNECTED	0/0

Icons beside each entry indicate the type of security gateway:

Individual security gateway

Security gateway group

2 Click **New.**



3 In Security Gateway dialog box, on the Gateway tab, in the IP address text box, type the IP address or fully qualified domain name of the security gateway.

Use either a true dotted decimal IP address or a resolvable DNS name.

4 Uncheck **Download VPN Policy.**

Note: If your administrator has not provided IKE policy, VPN policy, or tunnel information, the security gateway will autodownload this information. Complete the procedure in "Configuring for connections that support autodownload of VPN policies and tunnel information" on page 50.

---

5 If you want this security gateway to automatically connect each time you start Symantec Client VPN, check **Auto-connect on Client VPN start up.**

6 Under Client Information, select one of the following authentication methods:

- Certificate

  To use Certificate authentication, you must copy an Entrust X.509 digital certificate to the \ClientVPN directory, and you must configure Symantec Client VPN to use the certificate before you can use it to make a connection. See "Using digital certificates" on page 147.

- Shared secret

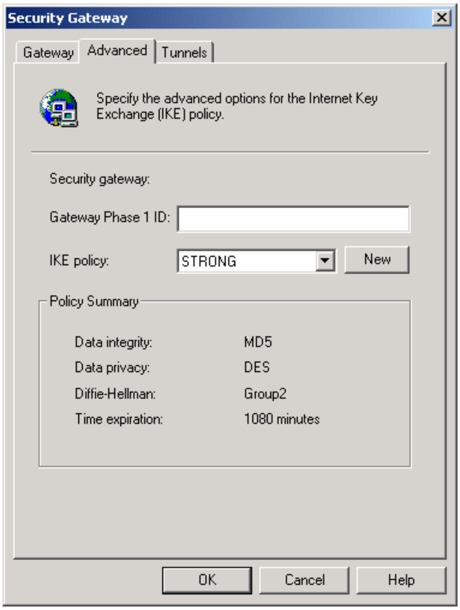
  If you select Shared secret, in the text box beside the option button, type the shared secret key that is provided by your administrator.

  Note that a shared secret that begins with the value "0x" is interpreted as a hexidecimal string if it consists of an even number of characters and is between 40 and 128 characters in length.

7 In the Client Phase 1 ID text box, type the Client Phase 1 ID that is provided by your administrator.

This may be your user name as it is configured at the security gateway, or your user name for extended authentication.

8 If you have been given a Gateway Phase 1 ID, on the Advanced tab, in the Gateway Phase 1 ID text box, type the value.



Specify the advanced options for the Internet Key Exchange (IKE) policy.

Security gateway:

Gateway Phase 1 ID:

IKE policy: STRONG

Policy Summary

Data integrity:	MD5
Data privacy:	DES
Diffie-Hellman:	Group2
Time expiration:	1080 minutes

The Gateway Phase 1 ID, also known as the Remote Phase 1 ID, should be the same as the security gateway Phase 1 ID. It is the identifier that lets phase 1 negotiations move forward.

If you do not type a string here, by default the IP address of the security gateway will be used as the Gateway Phase 1 ID.

9 If you have been given IKE policy details, you can specify them by using the IKE policy drop-down list to select an IKE policy.

The IKE policy is used to negotiate a phase 1 secure link between Symantec Client VPN and the security gateway.

Do one of the following:

- In the IKE policy drop-down list, select one of the predefined IKE policies: STRONG or VERY STRONG.

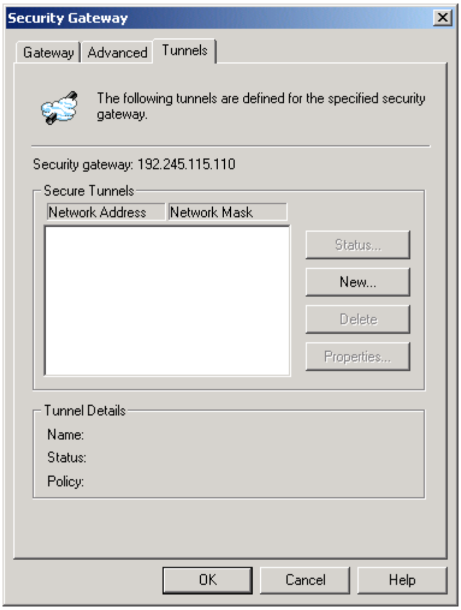
  For a description of the parameters of these policies, click **Help**.
- To define your own IKE policy, next to the IKE policy drop-down list, click **New**.

  See “Defining an IKE policy” on page 60.

Note: If you do not know which IKE policy to select, you can use the default, IKE STRONG. The phase 1 negotiation process will compare the policies on the security gateway and Symantec Client VPN and use the least restrictive algorithms to let the tunnel negotiation proceed.

The Policy Summary group box lists the parameters of the currently selected policy.

10 On the Tunnels tab, click **New**.



Security Gateway

The following tunnels are defined for the specified security gateway.

Security gateway: 192.245.115.110

11 In the Secure Tunnels dialog box, define the secure tunnels that are included in this security gateway, as described in “Adding a secure tunnel” on page 63.

12 Click **OK**.

Symantec Client VPN adds the security gateway to its database.

Defining an IKE policy

An IKE policy lets Symantec Client VPN create a secure link with a security gateway. Then, using the secure link, Symantec Client VPN can negotiate IPsec tunnels.

For options descriptions for the IKE Policy dialog box, click Help.

To define an IKE policy

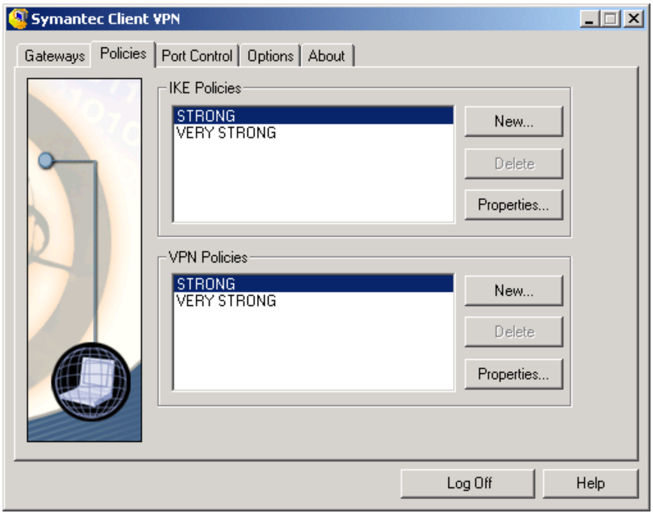
You can define an IKE policy:

- From the Policies tab of the Symantec Client VPN dialog box
- While you are configuring a new security gateway, by using the Advanced tab of the Security Gateway dialog box

Note: If you are editing an existing security gateway, and want to define a new IKE policy, you must use the Policies tab to define it, then choose it from the IKE policies list on the Advanced tab to add it to the security gateway.

To define an IKE policy from the Policies tab

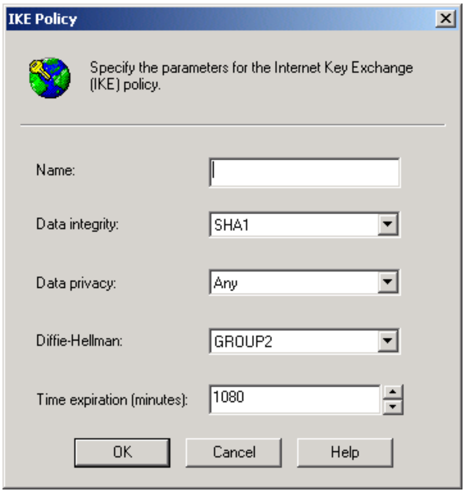
1 In the Symantec Client VPN dialog box, click the Policies tab.



STRONG
VERY STRONG

STRONG
VERY STRONG

2 In the IKE Policies group box, click **New**.



IKE Policy

Specify the parameters for the Internet Key Exchange (IKE) policy.

Name:

Data integrity: SHA1

Data privacy: Any

Diffie-Hellman: GROUP2

Time expiration (minutes): 1080

3 In the IKE Policy dialog box, define the algorithms that will be used for phase 1 negotiations.

Do the following:

Name

Type a name to identify the new IKE policy.

You can use up to 31 characters.

Data integrity

Select the type of authentication used on the tunnel data.

Data privacy

Select the type of encryption used on the tunnel data.

Diffie-Hellman

Select the key exchange method used to generate the keys for phase 1 and phase 2 negotiations.

Time expiration

Type or select the number of minutes you want the shared key to be valid for phase 1 negotiations.

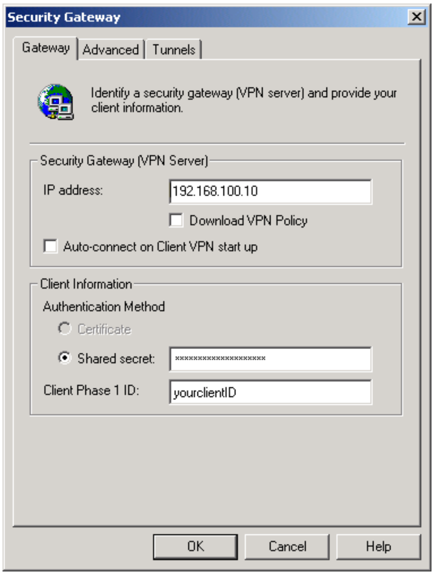
The default value is 1080 minutes (18 hours).

4 Click **OK**.

To define an IKE policy while configuring a security gateway

1 Create a new security gateway as described in "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

2 In the Security Gateway dialog box, on the Gateway tab, make sure that **Download VPN Policy** is not checked.



Identify a security gateway (VPN server) and provide your client information.

Security Gateway (VPN Server)

IP address: 192.168.100.10

□ Download VPN Policy

□ Auto-connect on Client VPN start up

Client Information

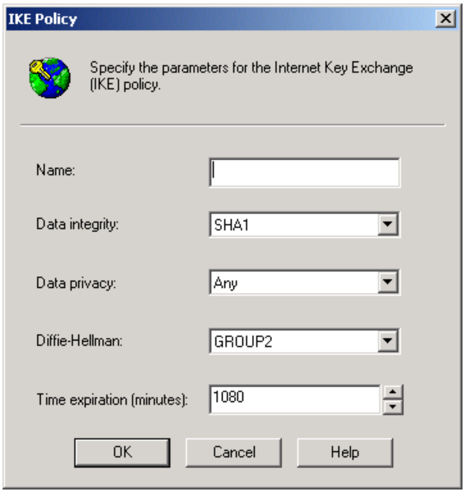
Authentication Method

○ Certificate

● Shared secret: ********************

Client Phase 1 ID: yourclientID

3 On the Advanced tab, beside the IKE Policy drop-down list, click **New**.



Specify the parameters for the Internet Key Exchange (IKE) policy.

Name:

Data integrity: SHA1

Data privacy: Any

Diffie-Hellman: GROUP2

Time expiration (minutes): 1080

4 In the IKE Policy dialog box, define the IKE policy as described in steps 3 and 4 of the previous procedure.

Viewing or editing an IKE policy

You can view the parameters for any IKE policy. However, you can only edit the parameters for a user-defined IKE policy.

To view or edit an IKE policy

1 In the Symantec Client VPN dialog box, on the Policies tab, in the IKE Policies group box, do one of the following:

- Select the IKE policy that you want to view, and then click **Properties**.
- Double-click the IKE policy that you want to view.

2 In the IKE Policy dialog box, use the drop-down list boxes to change the security algorithms.

Note: For options descriptions in the IKE Policy dialog box, click Help to view the Symantec Client VPN Online Help system.

If the IKE policy is one of the predefined policies (STRONG or VERY STRONG), you can view the parameters but you cannot change them.

Deleting an IKE policy

You can delete an IKE policy that you have created and are no longer using.

If the policy is in use by any security gateway, you cannot delete it. In addition, you cannot delete the predefined IKE policies: STRONG and VERY STRONG.

To delete an IKE policy

1 On the Policies tab, in the IKE policies section, select the IKE policy that you want to delete.

2 On the right side of the Policies tab, click **Delete**.

Adding a secure tunnel

When you connect to a security gateway, Symantec Client VPN establishes secure tunnels between your computer and the security gateway.

If the security gateway to which you connect does not support the autodownload of VPN policies and tunnel information, you must define a VPN policy and tunnel information when you configure the security gateway on Symantec Client VPN. You can also add additional configurations by editing the properties of an existing security gateway.

When you add a secure tunnel, you define the protected network behind the security gateway and a matching VPN policy. Your system administrator must provide the following information:

- The network address of the protected network or networks behind the security gateway
- The netmask of the protected network
- The details of the VPN policy for the security gateway

To add a secure tunnel

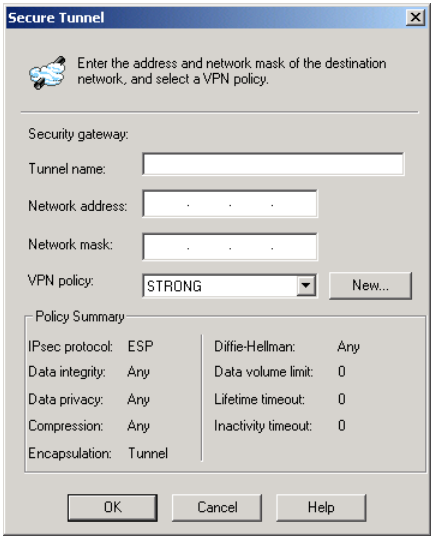
1 In the Symantec Client VPN dialog box, on the Gateways tab, do one of the following:

   - To add a secure tunnel to a new security gateway, click **New**.

     Specify the IP address and authentication information for the security gateway as described in "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

   - To add a secure tunnel to an existing security gateway, select the security gateway and click **Properties**.

2 On the Tunnels tab, click **New**.



Enter the address and network mask of the destination network, and select a VPN policy.

Security gateway:

Tunnel name:

Network address: . . .

Network mask: . . .

VPN policy: STRONG

Policy Summary

IPsec protocol:	ESP	Diffie-Hellman:	Any
Data integrity:	Any	Data volume limit:	0
Data privacy:	Any	Lifetime timeout:	0
Compression:	Any	Inactivity timeout:	0
Encapsulation:	Tunnel		

3 The Secure Tunnel dialog box lets you define a secure tunnel and the VPN policy that will be used by the secure tunnel.

Do the following:

Tunnel name

Type a name for the secure tunnel.

You can use up to 63 characters.

Network address

Type the IP address of the protected network behind the security gateway.

The IP address must be a true dotted decimal IP address, not a DNS resolvable name.

Network mask

Type the protected network's mask.

Similar to an IP address, the network mask defines how the assigned address space is split between hosts and networks.

VPN policy

To specify a VPN policy that matches the VPN policy of the security gateway to which you will connect, do one of the following:

- To select an existing VPN policy for the secure tunnel, use the VPN policy drop-down list.
  The predefined policies are STRONG and VERY STRONG. To display the Symantec Client VPN Help for the parameters for these policies, click **Help**.
- To define a new VPN policy, click **New**.
  Use the VPN Policy dialog box to create a new VPN policy as described in "Defining a VPN policy" on page 66. When finished, click **OK**.

The Policy Summary group box shows the IPsec parameters for the currently selected VPN policy.

Note: For descriptions of the parameters in the Policy Summary group box, click **New**. On each tab of the VPN Policy dialog box, to view the Symantec Client VPN Help for the parameters on that tab, click **Help**.

4. Click **OK**.

Defining a VPN policy

VPN policies define the combination of encapsulation, encryption, authentication and negotiation policies that are required for phase 2 negotiations for VPN connections. Phase 2 negotiations determine the protocol security association for the secure tunnel.

To view an explanation of your choices on each tab of the VPN Policy dialog box, click Help.

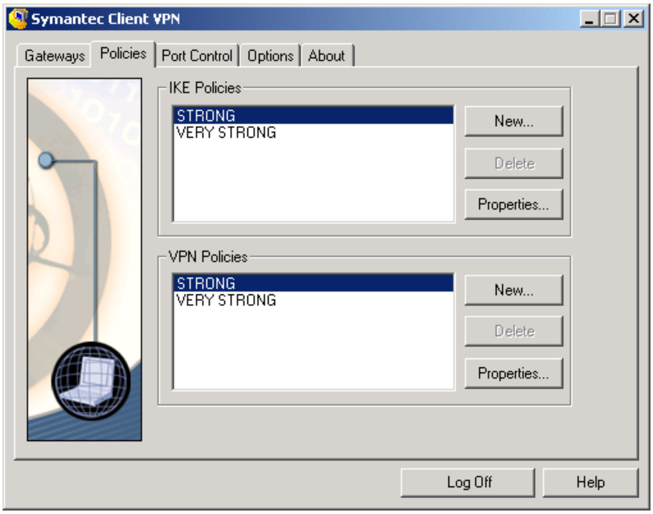
To define a VPN policy

You can define a VPN policy in two ways:

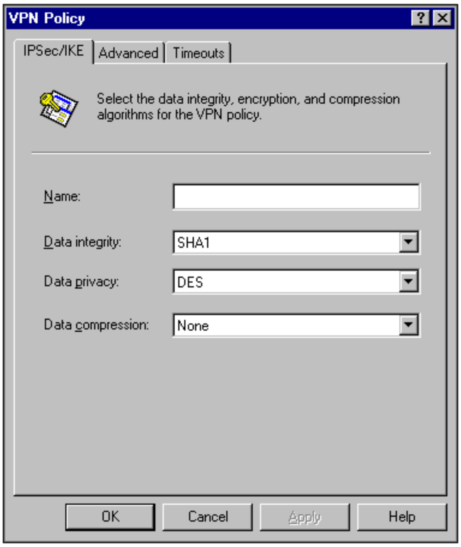
- From the Policies tab of the Symantec Client VPN dialog box
- While you are configuring a security gateway, by using the Tunnels tab of the Security Gateway dialog box

To define a VPN policy from the Policies tab

1 In the Symantec Client VPN dialog box, click the Policies tab.



2 In the VPN Policies group box, click **New**.



Select the data integrity, encryption, and compression algorithms for the VPN policy.

Name:

Data integrity: SHA1

Data privacy: DES

Data compression: None

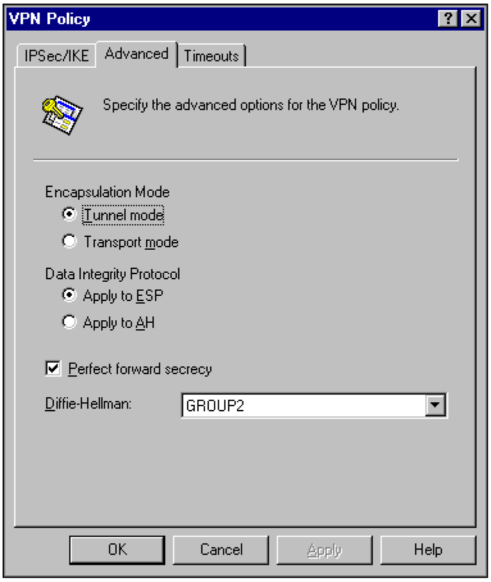
Use the VPN Policy dialog box to select the algorithms for the VPN policy.

3 The IPsec/IKE tab lets you specify algorithms used by the IKE-negotiated IPsec tunnel.

Do the following:

Name	Type a name for the VPN policy, using up to 31 characters.
Data integrity	Select the authentication type.
Data privacy	Select the encryption type.
Data compression	Select the compression type.

4 Click the Advanced tab.



Specify the advanced options for the VPN policy.

Encapsulation Mode

● Tunnel mode

○ Transport mode

Data Integrity Protocol

● Apply to ESP

○ Apply to AH

☑ Perfect forward secrecy

Diffie-Hellman: GROUP2

Do the following:

Encapsulation Mode
Select the Encapsulation Mode used on the data that is sent through the secure tunnel.

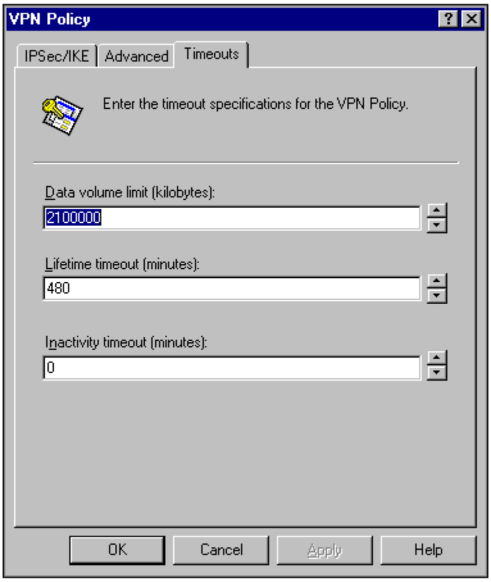
Data Integrity Protocol
Select the Data Integrity Protocol (that is, the type of IPsec header) in which the data integrity algorithm is included.

Perfect Forward secrecy
Select if you want to set up the parameters for generating keys and for preventing attackers from guessing successive keys.

If you check Perfect forward secrecy, you must specify a Diffie-Hellman group for the key exchange.

Diffie-Hellman
Select the key exchange method used to generate the keys for phase 2 negotiations.

5 Click the Timeouts tab.



Enter the timeout specifications for the VPN Policy.

Data volume limit (kilobytes): 2100000

Lifetime timeout (minutes): 480

Inactivity timeout (minutes): 0

Do the following:

Data volume limit (kilobytes)

Type or select the number of kilobytes of data that you want to let through the secure tunnel before it is rekeyed.

The default is 2100000 kilobytes (2.1 gigabytes).

Lifetime timeout (minutes)

Type or select the number of minutes that you want to let the secure tunnel exist before it is rekeyed.

The default is 480 minutes, (eight hours).

Inactivity timeout (minutes)

Type or select the number of minutes that you want to let the secure tunnel remain inactive (that is, have no data passing through it) before it is rekeyed.

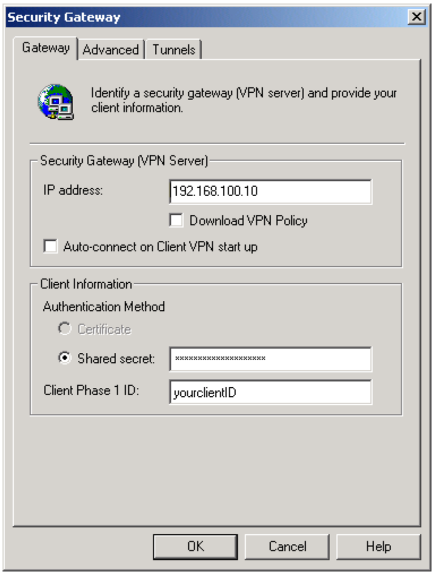
The default is 0 minutes, which means that the timeout is not used.

6 Click **OK**.

To define a VPN policy while configuring a security gateway

1. Create a new security gateway as described in "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

2. In the Security Gateway dialog box, on the Gateway tab, make sure that **Download VPN Policy** is not checked.



Security Gateway

Gateway | Advanced | Tunnels

Identify a security gateway (VPN server) and provide your client information.

Security Gateway (VPN Server)

IP address: 192.168.100.10

□ Download VPN Policy

□ Auto-connect on Client VPN start up

Client Information

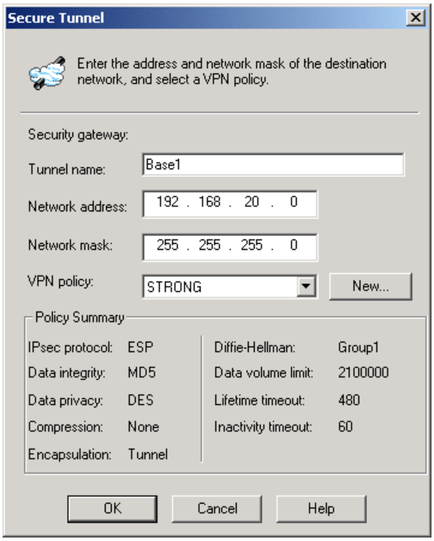
Authentication Method

○ Certificate

● Shared secret: ********************

Client Phase 1 ID: yourclientID

3 On the Tunnels tab, click **New.**



Secure Tunnel

Enter the address and network mask of the destination network, and select a VPN policy.

Security gateway:

Tunnel name: Base1

Network address: 192 . 168 . 20 . 0

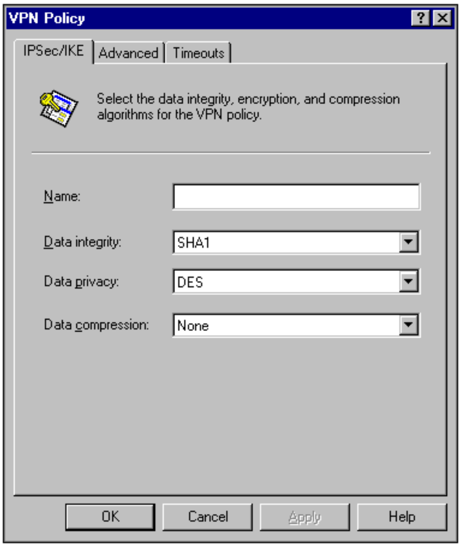
Network mask: 255 . 255 . 255 . 0

VPN policy: STRONG

Policy Summary

IPsec protocol:	ESP	Diffie-Hellman:	Group1
Data integrity:	MD5	Data volume limit:	2100000
Data privacy:	DES	Lifetime timeout:	480
Compression:	None	Inactivity timeout:	60
Encapsulation:	Tunnel		

4 In the Secure Tunnel dialog box, beside the VPN policy drop-down list, click **New.**



VPN Policy

Select the data integrity, encryption, and compression algorithms for the VPN policy.

Name:

Data integrity: SHA1

Data privacy: DES

Data compression: None

5 Use the VPN Policy dialog box to select the algorithms for the VPN policy as described in steps 3 through 6 of the previous procedure.

Viewing or editing a VPN policy

You can view the parameters for any VPN policy. However, you can only edit the parameters for a user-defined VPN policy.

To view or edit a VPN policy

1. In the Symantec Client VPN dialog box, on the Policies tab, in the VPN Policies group box, do one of the following:
   - Select the VPN policy that you want to view, and then click **Properties**.
   - Double-click the VPN policy that you want to view.
2. In the VPN Policy dialog box, view the policy parameters.

   Note: For description of the parameters on each tab of the VPN Policy dialog box, click **Help** to view an explanation of the parameters on that tab.

3. If you are viewing a user-defined VPN policy, you can edit the policy parameters as needed.

   You cannot edit the pre-defined STRONG and VERY STRONG policies.

Deleting a VPN Policy

You can delete a VPN policy that you have created and that you are no longer using.

If the policy is in use by any secure tunnel, you cannot delete it. In addition, you cannot delete the pre-defined STRONG and VERY STRONG policies.

To delete a VPN policy

1. On the Policies tab, in the VPN policies section, select the VPN policy that you want to delete.
2. On the right side of the Policies tab, click **Delete**.

Viewing security gateway properties

To see the connection information for a security gateway you have defined, you can view its properties.

To view security gateway properties

1. On the Gateways tab, under Security Gateways, select the security gateway whose properties you want to view, and then click **Properties**.
2. Use the tabs of the Security Gateway dialog box to view the properties assigned to the security gateway.

Viewing secure tunnel properties and status

When you connect from Symantec Client VPN to a security gateway, the connection uses secure tunnels to securely pass data.

How you view the properties and status of secure tunnels, and whether you can make any changes to the secure tunnels, depends on the kind of security gateway those secure tunnels are associated with:

- If the security gateway is configured to support the download of VPN policies and tunnel information, you must connect to the security gateway before you can view tunnel information. See “Connecting to a security gateway using default connection settings” on page 88.

  When you connect, the information for the secure tunnels is downloaded from the security gateway. You can view the status of the connected secure tunnel as described in “Viewing secure tunnel status” on page 74.

  Note: You cannot change this information. Any changes must be made on the security gateway by the security gateway administrator.

- If you have used Symantec Client VPN to supply the tunnel information for the security gateway, you can view this information whether you are connected or not.

  The actions you can perform are described in:

  - “Viewing secure tunnel status” on page 74
  - “Viewing or editing secure tunnel properties” on page 76
  - “Deleting a secure tunnel” on page 78

Viewing secure tunnel status

If you configure a security gateway to autodownload tunnel information, you can view information about the status of downloaded tunnels only when you are connected to the security gateway.

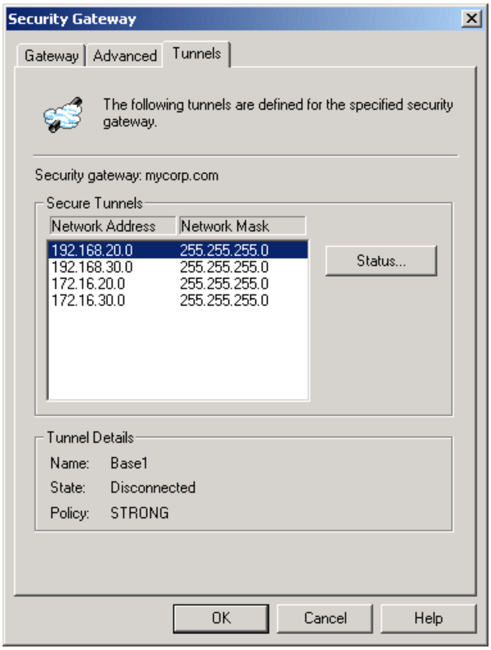
If you configure the secure tunnels for your security gateway, you can view tunnel status at any time.

To view secure tunnel status

1 If the security gateway supports the autodownload of VPN policies and tunnel information, connect as described in "Connecting to a security gateway using default connection settings" on page 88.

If you have defined the secure tunnel, you do not have to connect to see its status.

2 In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway associated with the secure tunnel whose properties you want to view, and then click **Properties**.



The following tunnels are defined for the specified security gateway.

Security gateway: mycorp.com

Secure Tunnels

Network Address	Network Mask
192.168.20.0	255.255.255.0
192.168.30.0	255.255.255.0
172.16.20.0	255.255.255.0
172.16.30.0	255.255.255.0

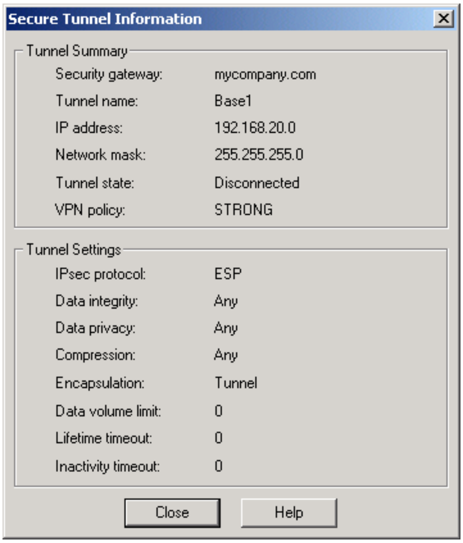
Tunnel Details

Name: Base1
State: Disconnected
Policy: STRONG

3 On the Tunnels tab, select a secure tunnel.

The Tunnel Details section displays the secure tunnel name, its current state, and the VPN policy associated with the secure tunnel.

4 Click **Status.**



Tunnel Summary

Security gateway: mycompany.com
Tunnel name: Base1
IP address: 192.168.20.0
Network mask: 255.255.255.0
Tunnel state: Disconnected
VPN policy: STRONG

Tunnel Settings

IPsec protocol: ESP
Data integrity: Any
Data privacy: Any
Compression: Any
Encapsulation: Tunnel
Data volume limit: 0
Lifetime timeout: 0
Inactivity timeout: 0

The Secure Tunnel Information dialog box displays the parameters being used for the selected secure tunnel. The information in the dialog box is read-only.

- The Tunnel Summary section shows either the values supplied when the secure tunnel was downloaded, or the values you supplied when you created the secure tunnel.

  It also includes the Tunnel state.

- The Tunnel Settings section describes the algorithms used for the VPN policy.

  To view these parameters, click **Help.**

5 To return to the Tunnels dialog box, click **Close.**

Viewing or editing secure tunnel properties

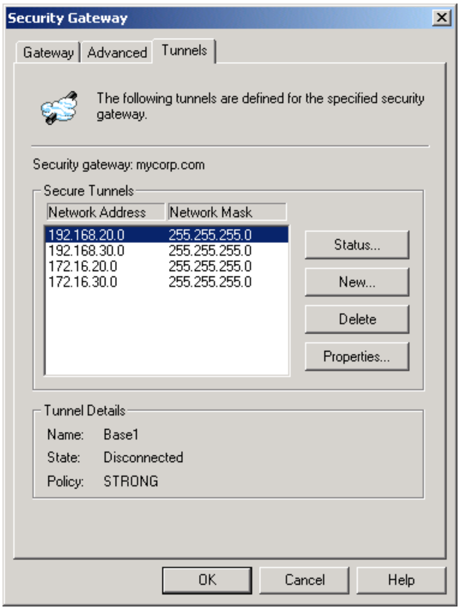
If you define the tunnel information for your security gateway, you can view the properties of the secure tunnels.

If you create a security gateway that supports the autodownload of VPN policies and tunnel information, you cannot view or change the properties of secure tunnels that are downloaded.

To view secure tunnel properties

1 In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway associated with the secure tunnel whose properties you want to view, and then click **Properties**.

2 On the Tunnels tab, from the Secure Tunnels list, select a secure tunnel.



The following tunnels are defined for the specified security gateway.

Security gateway: mycorp.com

Secure Tunnels

Network Address	Network Mask
192.168.20.0	255.255.255.0
192.168.30.0	255.255.255.0
172.16.20.0	255.255.255.0
172.16.30.0	255.255.255.0

Tunnel Details

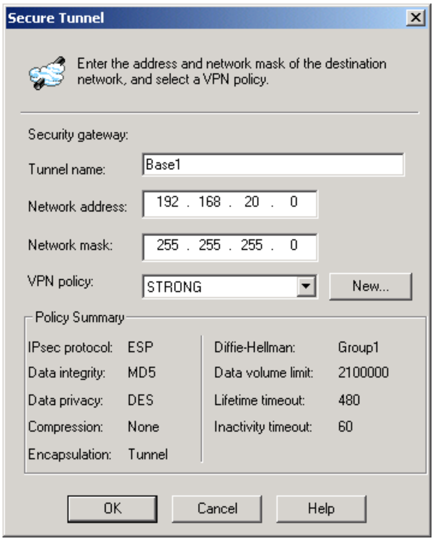
Name: Base1

State: Disconnected

Policy: STRONG

The Tunnel Details section displays the tunnel name, its current state, and the VPN policy associated with the secure tunnel.

3 To view additional details for the secure tunnel, click **Properties.**



Secure Tunnel

Enter the address and network mask of the destination network, and select a VPN policy.

Security gateway:

Tunnel name: Base1

Network address: 192 . 168 . 20 . 0

Network mask: 255 . 255 . 255 . 0

VPN policy: STRONG

Policy Summary

IPsec protocol:	ESP	Diffie-Hellman:	Group1
Data integrity:	MD5	Data volume limit:	2100000
Data privacy:	DES	Lifetime timeout:	480
Compression:	None	Inactivity timeout:	60
Encapsulation:	Tunnel		

In the Secure Tunnel dialog box, the text boxes show the IP address and netmask of the protected network behind the security gateway, and the VPN policy used to negotiate the secure tunnel.

4 The Policy Summary section shows the IPsec parameters of the VPN policy. For a description of these parameters, do the following:

- Click **New.**
- On each tab of the VPN Policy dialog box, click **Help** to view an explanation of the parameters that can be selected using that tab.

5 To return to the Security Gateway dialog box, click **OK**.

Deleting a secure tunnel

You can only delete secure tunnels that have been configured for security gateways that do not support the autodownload of VPN policies and tunnel information.

To delete a secure tunnel

1. In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway associated with the secure tunnel that you want to delete, and then click **Properties**.
2. On the Tunnels tab, from the Secure Tunnels list, select the secure tunnel you want to delete.
3. Beside the Secure Tunnels list, click **Delete**.

Deleting a security gateway

You can delete security gateways that you are no longer using; however, you cannot delete a security gateway that is connected.

You may also need to delete a security gateway if you want to add it to a different security gateway group, since you can only define a specific security gateway once.

To delete a security gateway

1. In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway that you want to delete.
2. Beside the Security Gateways list, click **Delete**.
3. When asked to confirm the deletion, do one of the following:
   - To delete the security gateway, click **Yes**.
   - To leave the security gateway, click **No**.

Configuring and connecting security gateway groups

After you log on, you can configure security gateway groups that you will use to connect to your remote resources. You can group security gateway entries together and represent them with a single name.

When you use a security gateway group to connect, each security gateway in the group is tried until you get a successful connection.

You create a security gateway group by naming the group and then configuring the individual security gateways that make up the group. The methods you use to configure the security gateways are the same as those that are described in "Configuring for connections that support autodownload of VPN policies and tunnel information" on page 50 and "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

Note: If you have already configured a security gateway, you must delete it before you can use it in a gateway group.

This chapter includes the following topics:

- Configuring a security gateway group
- Connecting using a security gateway group
- Disconnecting a security gateway

Configuring a security gateway group

A security gateway group is a set of security gateways. When you configure a security gateway group and use it to connect, each security gateway in the group is tried until a successful connection is made.

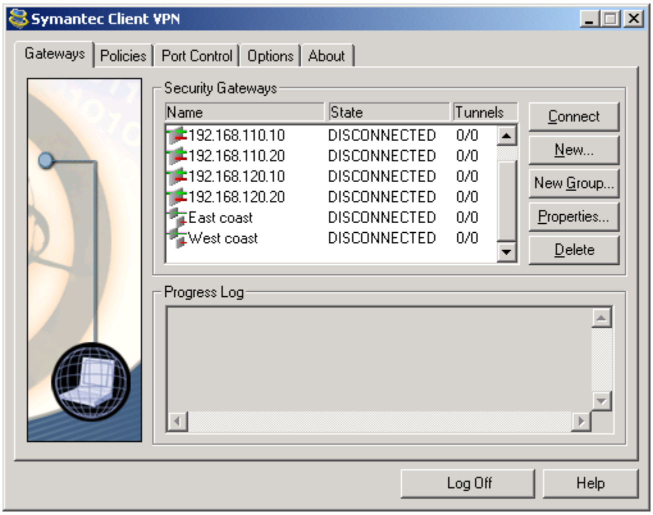
You can configure a security gateway group to connect to Symantec security gateways that support autodownload of VPN policies and tunnel information and to security gateways that do not support autodownload of VPN policies and tunnel information.

All security gateways defined on Symantec Client VPN must be unique. If you have already configured a security gateway and want to use it in a security gateway group, you must delete it from the Security Gateways list on the Gateways tab before you can recreate it within a security gateway group. See “Deleting a security gateway” on page 78.

To configure a security gateway group

1 Log on to Symantec Client VPN.

The Gateways tab shows the security gateways and security gateway groups that you have already defined.



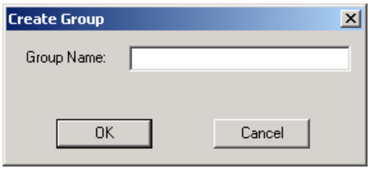
Name	State	Tunnels
192.168.110.10	DISCONNECTED	0/0
192.168.110.20	DISCONNECTED	0/0
192.168.120.10	DISCONNECTED	0/0
192.168.120.20	DISCONNECTED	0/0
East coast	DISCONNECTED	0/0
West coast	DISCONNECTED	0/0

Icons beside each entry indicate the type of security gateway:

Individual security gateway

Security gateway group

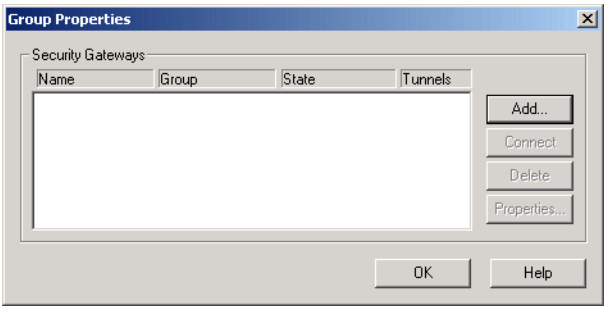
2 Click **New Group**.



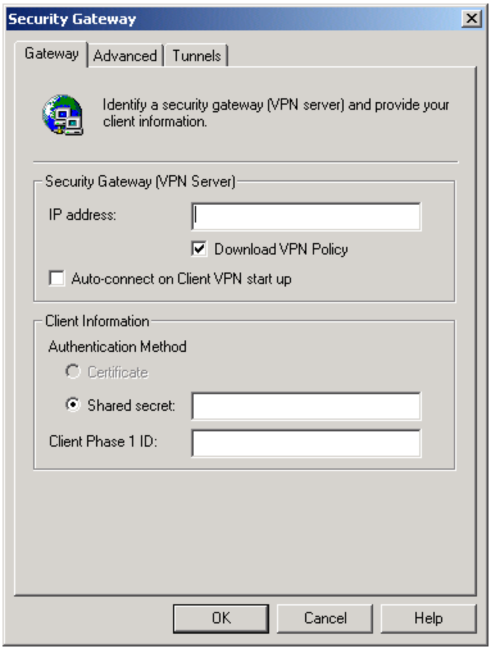
3 In the Create Group dialog box, in the Group Name text box, type a name for the security gateway group.

You can make this name descriptive so that it is easy to identify the security gateways that the group will contain.

4 Click **OK**.



5 In the Group Properties dialog box, click **Add**.



Identify a security gateway (VPN server) and provide your client information.

Security Gateway (VPN Server)

IP address:

☑ Download VPN Policy

□ Auto-connect on Client VPN start up

Client Information

Authentication Method

○ Certificate

● Shared secret:

Client Phase 1 ID:

6 In the Security Gateway dialog box, complete the creation of the security gateway as described in one of the following:

- "Configuring for connections that support autodownload of VPN policies and tunnel information" on page 50.
- "Configuring for connections that do not support autodownload of VPN policies and tunnel information" on page 54.

7 When you finish configuring the security gateway, click **OK**.

The security gateway is added to the list in the Group Properties dialog box.

Note: As you add security gateways to a security gateway group, they are listed in alphabetical order.

8 To add additional security gateways, repeat steps 5 through 7.

Viewing security gateway properties in a security gateway group

To see the connection information for a security gateway in a security gateway group, you can view its properties.

To view security gateway properties in a security gateway group

1. In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway group that contains the security gateway, and then click **Properties**.
2. In the Gateway Properties dialog box, select the security gateway, then click **Properties**.
3. Use the tabs of the Security Gateway dialog box to view the properties assigned to the security gateway.

Deleting a security gateway from a security gateway group

You can delete security gateways that you are no longer using; however, you cannot delete a security gateway that is connected.

You must also delete a security gateway if you want to add it to a different security gateway group, since you can only define a specific security gateway once.

Deleting the last security gateway from a security gateway group deletes the security gateway group.

To delete a security gateway from a security gateway group

1. In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway group that contains the security gateway that you want to delete, and then click **Properties**.
2. On the Group Properties tab, select the security gateway.
3. Beside the Security Gateways list, click **Delete**.
4. When asked to confirm the deletion, do one of the following:
   - To delete the security gateway, click **Yes**.
   - To leave the security gateway, click **No**.

Connecting using a security gateway group

When you configure a security gateway group and use it to connect, each security gateway in the group is tried until a successful connection is made.

If the end of the list is reached and no connection was made, you can try to connect again using the same security gateway group, or try another security gateway group or security gateway.

To connect using a security gateway group

There are two ways you can connect when your security gateways are defined in security gateway groups.

- Connect by selecting a security gateway group and clicking Connect. In this case, each security gateway in the group is tried in the order in which the security gateways are listed until a successful connection is made. Only one security gateway from the group is actually connected.
- Connect directly to a specific security gateway by displaying the properties of the security gateway group and selecting the security gateway.

To connect at the group level

1. On the Gateways tab, under Security Gateways, select a security gateway group.
2. Click **Connect**.

   Symantec Client VPN will try each security gateway, in alphabetical order, until it makes a successful connection.
3. If you want to interrupt the connection process, click **Disconnect**.

   Note: The Connect button changes to Disconnect when the connection attempt begins.

To connect using a specific security gateway in a security gateway group

1. On the Gateways tab, under Security Gateways, select the security gateway group, and then click **Properties**.
2. In the Group Properties dialog box, do one of the following:
   - Select a specific security gateway, and then click **Connect**.
   - Double-click a specific security gateway.

   Symantec Client VPN will attempt a connection to the specified security gateway. If that connection fails, it will not attempt another connection.

Disconnecting a security gateway

When you have finished using your remote resources, you can disconnect your security gateway.

Note: Symantec Client VPN disconnects automatically if it does not detect any activity within a specified time period, a network adapter changes, or a security gateway is unreachable.

See "Setting the time for disconnecting inactive tunnels" on page 93.

However, continuous WINS and DNS activity that occurs in the background may prevent Symantec Client VPN from automatically disconnecting.

To disconnect a security gateway

◆ Do one of the following:

- In the Symantec Client VPN dialog box, on the Gateways tab, select the security gateway group, and then click **Disconnect**.
- Double-click the security gateway group that you want to disconnect.
- In the Symantec Client VPN dialog box, click **Log Off**.

  When asked if you want to disable all tunnels, click **Yes**.
- Right-click on the Symantec Client VPN icon in the Microsoft Windows system tray,

  Click the connected security gateway that you want to disconnect.

Symantec Client VPN closes the secure tunnels that are associated with the security gateway, disconnects the security gateway, and removes the secure link to the host. The Progress Log shows the changes.

Although you are disconnected, the security gateway configuration parameters remain in the Symantec Client VPN database.

Chapter 6

Connecting to a security gateway

When you have configured your security gateways, you can use them to establish a secure, tunneled connection to your private network.

- If you connect to a Symantec security gateway, the tunnel information for the connection is autodownloaded to Symantec Client VPN.
- If you connect to a security gateway that does not support the autodownload of tunnel information by Symantec Client VPN, the secure tunnels that you have defined will be used for the connection.

You remain connected until you choose to disconnect or until your secure tunnels time out because of inactivity.

You can set the inactivity timeout and other connection options.

This chapter includes the following topics:

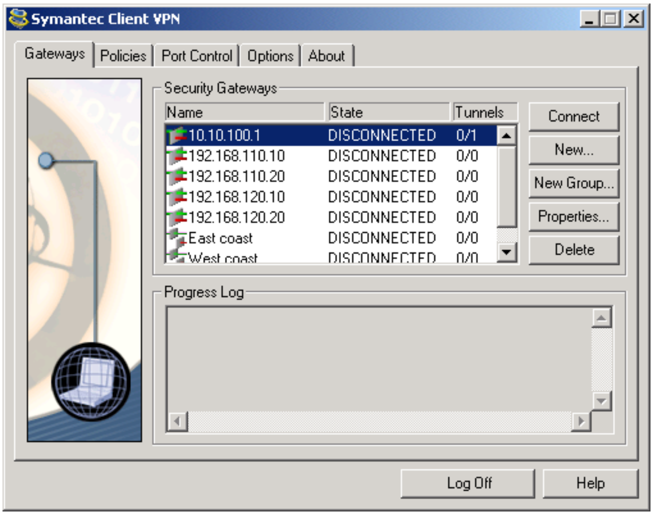
Connecting to a security gateway using default connection settings

A security gateway connects Symantec Client VPN with your protected remote resources.

You can connect to security gateways using default Symantec Client VPN connection settings. If you want to customize the behavior of your computer when you connect or have problems connecting, see “Configuring connection options” on page 91.

To connect to a security gateway using default connection settings

1 On the Gateways tab, under Security Gateways, select the security gateway to which you want to connect.



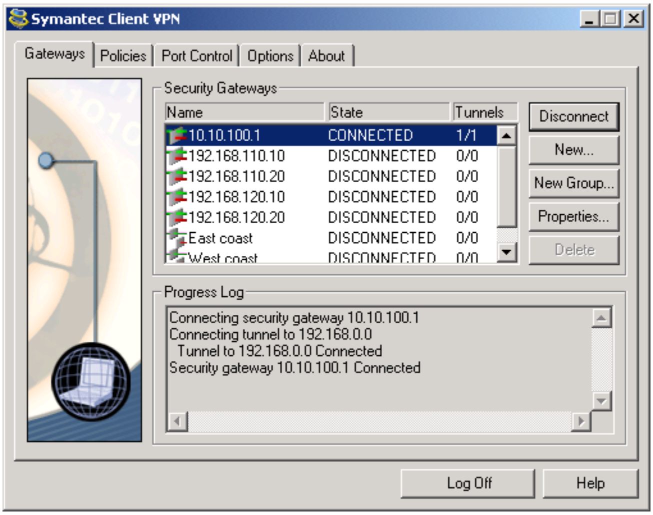
Name	State	Tunnels
10.10.100.1	DISCONNECTED	0/1
192.168.110.10	DISCONNECTED	0/0
192.168.110.20	DISCONNECTED	0/0
192.168.120.10	DISCONNECTED	0/0
192.168.120.20	DISCONNECTED	0/0
East coast	DISCONNECTED	0/0
West coast	DISCONNECTED	0/0

2 Do one of the following:

- Click **Connect**.
- Double-click the selected security gateway.

Symantec Client VPN attempts to connect to the selected security gateway.

Note: If your security gateway is configured to use extended user authentication, you may be prompted to provide additional authentication information before the security gateway connects.



Name	State	Tunnels
10.10.100.1	CONNECTED	1/1
192.168.110.10	DISCONNECTED	0/0
192.168.110.20	DISCONNECTED	0/0
192.168.120.10	DISCONNECTED	0/0
192.168.120.20	DISCONNECTED	0/0
East coast	DISCONNECTED	0/0
West coast	DISCONNECTED	0/0

```
Connecting security gateway 10.10.100.1
Connecting tunnel to 192.168.0.0
  Tunnel to 192.168.0.0 Connected
Security gateway 10.10.100.1 Connected
```

After the security gateway connects, the following changes occur in the Gateways tab:

- The State column changes from DISCONNECTED to CONNECTING as the security gateway connects, and then to CONNECTED after the connection is complete.
- The Tunnels column updates to reflect the number of connected secure tunnels.
- The Connect button changes to Disconnect.
- The Progress Log displays the current session’s security gateway and tunnel activity, in real-time.

In addition, the Symantec Client VPN icon in the Windows system tray changes to show that you are connected.

If you have enabled Minimize on connect, the Symantec Client VPN window is minimized.

Disconnecting from a security gateway

When you have finished using your remote resources, you can disconnect your security gateway.

Note: Symantec Client VPN disconnects automatically if it does not detect any activity within a specified time period, a network adapter changes, or a security gateway is unreachable.

See “Setting the time for disconnecting inactive tunnels” on page 93.

However, continuous WINS and DNS activity that occurs in the background may prevent Symantec Client VPN from automatically disconnecting.

To disconnect a security gateway

◆ Do one of the following:

- In the Symantec Client VPN window, on the Gateways tab, select the security gateway from which you want to disconnect, and then click **Disconnect**.
- Double-click the security gateway from which you want to disconnect.
- In the Symantec Client VPN window, click **Log Off**.

  When asked if you want to disable all tunnels, click **Yes**.
- Right-click on the Symantec Client VPN icon in the Windows system tray.

  Click the connected security gateway that you want to disconnect.

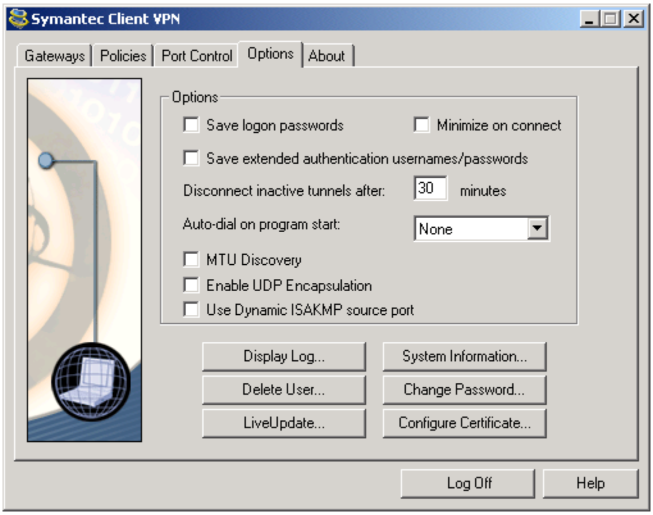
Symantec Client VPN closes the secure tunnels that are associated with the security gateway and disconnects the security gateway, and removes the secure link to the host. The Progress Log shows the changes.

Although you are disconnected, the security gateway configuration parameters remain in the Symantec Client VPN database.

Configuring connection options

Symantec Client VPN provides several options that control the behavior of the client when you make a connection to your security gateway. They are available on the Symantec Client VPN window Options tab.

Figure 6-1 Symantec Client VPN Options tab



Options

☐ Save logon passwords ☐ Minimize on connect

☐ Save extended authentication usernames/passwords

Disconnect inactive tunnels after: 30 minutes

Auto-dial on program start: None

☐ MTU Discovery

☐ Enable UDP Encapsulation

☐ Use Dynamic ISAKMP source port

Use the following procedures to customize your connections:

- Saving extended authentication user names and passwords
- Configuring Symantec Client VPN to minimize on connect
- Setting the time for disconnecting inactive tunnels
- Managing data packet sizes (MTU Discovery)
- Overcoming NAT connection problems

Saving extended authentication user names and passwords

If your connection requires the use of extended authentication, when you connect you are prompted to type your user name and, in some cases, password.

You can save your extended authentication user name and password, so that when you connect, instead of prompting you, Symantec Client VPN supplies the required information.

Caution: Saving passwords reduces the security of your system because anyone with access to your computer can log on as you and connect to your internal network.

To save extended authentication user names and passwords

1. In the Symantec Client VPN window, on the Options tab, under Options, check **Save extended authentication usernames/passwords**.
2. When you are warned that saving passwords can reduce the security of your system, do one of the following:
    - To save your passwords, click **Yes**.
    - To clear the Save extended authentication usernames/passwords check box, click **No**.
3. When you change tabs or log off, you are asked if you want to apply your preference changes. Do one of the following:
    - To apply any changes, click **Yes**.
    - To clear any changes, click **No**.

Configuring Symantec Client VPN to minimize on connect

You can configure Symantec Client VPN to minimize once a connection to a private network has been successfully established.

To minimize and redisplay Symantec Client VPN

When minimized, Symantec Client VPN is visible as an icon in the system tray in the lower right corner of the Microsoft Windows task bar. The application is still active, and your connection remains open.

To configure Symantec Client VPN to minimize on connect

1. In the Symantec Client VPN window, on the Options tab, under Options, check **Minimize on connect**.
2. When you change tabs or log off, you are asked if you want to apply your preference changes. Do one of the following:
   - To apply any changes, click **Yes**.
   - To clear any changes, click **No**.

To redisplay Symantec Client VPN on the desktop

◆ In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Open Symantec Client VPN**.

You can also redisplay Symantec Client VPN by double-clicking the system tray icon.

Setting the time for disconnecting inactive tunnels

Inactive secure tunnels are tunnels that have no data passing through them.

Symantec Client VPN secure tunnels are automatically disconnected when all tunnels have been inactive for a specified period of time. The default time period, which you can change, is 30 minutes.

Note: Continuous WINS and DNS activity that occurs in the background may prevent Symantec Client VPN from automatically disconnecting.

To set the time for disconnecting inactive tunnels

1. In the Symantec Client VPN window, on the Options tab, in the Disconnect inactive tunnels text box, type the number of minutes that you want to let secure tunnels remain inactive before they are disconnected.

   The default value is 30 minutes.
2. When you change tabs or log off, you are asked if you want to apply your preference changes. Do one of the following:
   - To apply any changes you have made, click **Yes**.
   - To clear any changes you have made, click **No**.

Managing data packet sizes (MTU Discovery)

The MTU (Maximum Transmission Unit) Discovery option lets you manage data packet sizes. You can apply this capability to any Internet service provider (ISP); however, it is most important for the connections that use Point-to-Point Protocol over Ethernet (PPPoE).

When you enable MTU Discovery, the correct MTU size for your current ISP connection is automatically calculated. If an adjustment is necessary, the calculated MTU size is displayed; the adjustment takes place after you restart your computer.

Enabling this option ensures that the correct MTU size is automatically calculated for the current connection. It has no effect on product compatibility with other PPPoE software (for example, WinPoet).

To automatically adjust data packet size

1. Connect to your ISP.
2. Log on to Symantec Client VPN.
3. In the Symantec Client VPN window, on the Options tab, check **MTU Discovery**.

   A screen message tells you the MTU that has been determined for your ISP, and instructs you to restart your computer.
4. Click **OK**.
5. To make the settings take effect, log off Symantec Client VPN and restart your computer.

To revert to your previous settings, uncheck MTU Discovery and restart your computer.

Overcoming NAT connection problems

When there is a NAT device or firewall between you and the security gateway, you may fail to connect or, after a successful connection, you may fail to pass any traffic.

A variety of scenarios can cause NAT connection problems:

- Routers and Network Address Translation (NAT) devices vary in their ability to handle IPsec and IKE traffic.

  Problems may occur if you are located at a hotel or other public broadband Internet access location or if you have purchased a router/NAT/firewall device for your home network.

  You can sometimes tell if you are behind a NAT device by the IP address that is assigned to you. These private addresses start with 192.168.x.x or 10.x.x.x or 172.16.x.x through 172.31.x.x.
- IPsec traffic may be blocked if there is a firewall between you and the security gateway.
- Your NAT device may not be able to handle fragmented IPsec packets.

  In this case small data traverses successfully but large data does not.

In all of these situations, your failure is not the result of authentication issues.

Two options are provided to workaround NAT device limitations:

- Enable UDP Encapsulation

  When Enable UDP Encapsulation is checked, if you are behind a NAT device, the packet framing is changed.

  Normally the outside framing is ESP or AH (IPsec). This framing is encapsulated into UDP packets to get through the NAT device. The server User Datagram Protocol (UDP) port is 786 and the client source port varies. UDP port 786 on the Symantec security gateway cannot be changed.

  Note: UDP destination port 786 must not be blocked by any device between you and the security gateway.

  If you are not behind a NAT device, UDP Encapsulation is not used even if the box is checked. In addition, UDP Encapsulation is not used if the security gateway does not support it.

- Use Dynamic ISAKMP source port

  Normally, the ISAKMP source port is 500. When checked, a random source port is used instead to start the secure connection. Very often a random source port is necessary when two Symantec Client VPNs are behind the same NAT box.

  The UDP destination port for ISAKMP is 500 by RFC standard and cannot be changed. This port must not be blocked by any device between you and the security gateway.

Both of these options require a Symantec security gateway that supports UDP encapsulation. By default, UDP encapsulation is not enabled.

You should not check these boxes unless you have a problem using standard IPsec and/or ISAKMP traffic. If you check Use Dynamic ISAKMP source port and your security gateway does not support this option, your tunnel may fail.

You can use these options individually or in combination.

To troubleshoot NAT related connection problems

1. In the Symantec Client VPN window, on the Options tab, check E**nable UDP Encapsulation** and/or **Use Dynamic ISAKMP source port**.
2. When you change tabs or log off, you are asked if you want to apply your preference change. Do one of the following:
   - To apply any changes you have made, click **Yes**.
   - To clear any changes you have made, click **No**.
3. Attempt to connect to the security gateway at least twice. If you continue to fail to pass data, you can try different check box combinations.

Chapter 7

Using port control for personal firewall protection

Symantec Client VPN provides personal firewall protection through default port control settings. You do not have to take any action to operate your Symantec Client VPN securely using these default settings.

If the security of your system is already guaranteed by its location behind another security gateway, you can use the features on the Port Control tab to control host access and enable connectivity with other computers in your local area network (LAN).

Note: Port control is not active inside of a secure tunnel. Port control settings do not apply to tunnel traffic: they only apply to traffic outside a secure tunnel.

Port control settings let you:

- Permit hosts to connect to you

  While you can always freely connect to whomever you choose, the port control settings let you control who can connect to you.

  No host can successfully connect to you on the Internet unless you initiate communications first. Furthermore, the Internet host must connect back within two minutes of the time you first connected to it.

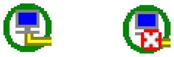
  Caution: Use sound judgement when browsing the Web and opening unknown mail. Always have Norton AntiVirus or Norton Internet Security checking email attachments and downloaded files.

- Enable file and print sharing

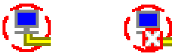
  You can enable file and print sharing for connectivity between computers on your local LAN segment. For example, when using a laptop computer in an office protected by a corporate security gateway, you can enable File/Print sharing. When using your laptop at home on the Internet, you should disable File/Print sharing.

  Because file and print sharing can be a security risk on the Internet without a security gateway, it is disabled by default.

The Symantec Client VPN icon in the Windows system tray indicates the status of your port control settings:



Protected, using port control defaults.



Unprotected: the port control type is set to Wide Open or file and print sharing is enabled.

This chapter includes the following topics:

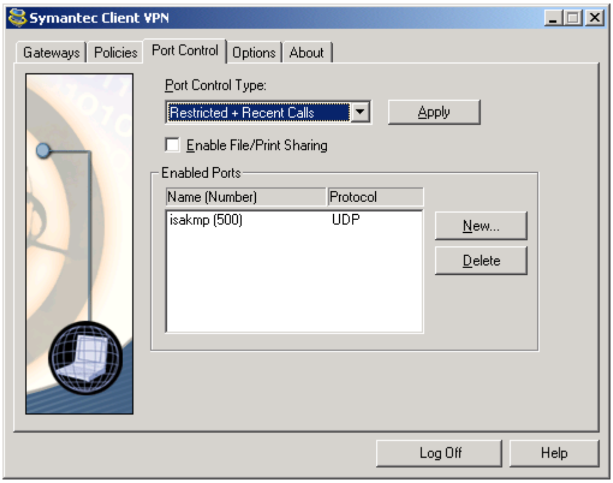
- About the Port Control options
- Selecting a type of port control
- Adding ports or IP protocols
- Deleting a port or IP protocol
- Enabling and disabling file and print sharing

About the Port Control options

The Symantec Client VPN personal firewall port control features let you configure the ports through which other hosts can connect to you.

Figure 7-1 shows the Port Controls tab, from which you configure ports.

Figure 7-1 Port Control tab



Port Control Type: Restricted + Recent Calls

□ Enable File/Print Sharing

Enabled Ports

Name (Number)	Protocol
isakmp (500)	UDP

You can control the amount of personal firewall protection you have by:

- Selecting a type of port control
- Adding ports or IP protocols
- Deleting a port or IP protocol
- Enabling and disabling file and print sharing

Any changes that you make take effect immediately and remain in effect until you change them back. Also, these are global settings that apply to all users of Symantec Client VPN on this system

Caution: Do not change default port control settings unless you are protected by another firewall or security gateway.

Use special caution if you change the port control settings on your laptop. Remember to restore secure port control settings when you leave a work area that is protected by another security gateway. Always make sure you are protected when you travel.

Selecting a type of port control

The type of port control you specify determines how an external address or Internet host can connect to you. The three available types are:

- Restricted and Recent Calls

  The default setting, Restricted + Recent Calls, limits traffic to designated ports, or to connections from external IP addresses to which you have recently sent traffic.

  No host can successfully connect to you on the Internet unless you initiate communications first. Furthermore, the Internet host must connect back within two minutes of the time you first connected to it.

- Wide Open

  You can use Wide Open if you do not want any port restrictions. This disables the personal firewall entirely so that all incoming packets are accepted.

  However, we recommend that you configure the personal firewall more selectively by opening up specific ports for specific reasons.

  Caution: Use this setting only if you are protected by another firewall or security gateway.

- Restricted

  Use Restricted to prevent any host from contacting you except using any ports that you have opened.

  You are still able to freely connect to whomever you choose.

  While this increases security, it can lead to connectivity problems. For example, the FTP protocol can stop working.

To select the port control type

1. Do one of the following to display the port control settings:
   - In the Symantec Client VPN window, click the **Port Control** tab.
   - In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Port Control**.
2. Use the Port Control Type drop-down list to select a port control type.
3. Click **Apply**.

   The Enabled Ports list shows the ports through which access is allowed.

Adding ports or IP protocols

You only need to add a port to Port Control if you wish to permit unsolicited requests from any host to the service represented by the port. This lets your computer act as a server on that port, allowing anyone to connect using the port.

You should avoid adding ports or IP protocols unless you are instructed to do so by your IT department. For example, you may be instructed to add port 2967 UDP to enable Symantec AntiVirus Corporate Edition to talk to Symantec Client VPN while your lap top is connected at work.

Caution: Do not add ports or IP protocols unless you are protected by another firewall or security gateway.

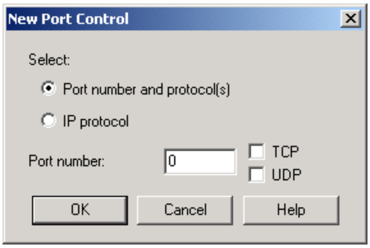
To add a port or IP protocol

The options displayed in the New Port Control dialog box vary depending on whether you are adding a port or an IP protocol.

To add a port number and protocol

1 On the Port Control tab, click **New**.

2 In the New Port Control dialog box, to add a port number through which you want data packets to be able to pass, click **Port number and protocols**.



New Port Control

Select:

● Port number and protocol(s)

○ IP protocol

Port number: 0

□ TCP

□ UDP

3 In the Port Number text box, type the port number through which you want the data packets to pass.

In the example of enabling the Symantec AntiVirus server to connect with the client, this would be 2967.

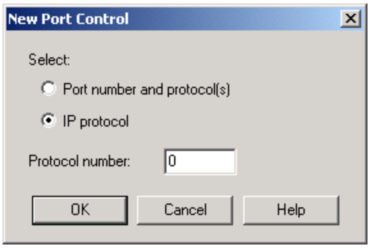
4. Select at least one type of protocol:
   - To accept the Transmission Control Protocol (TCP) on the specified port, select **TCP**.
   - To accept the User Datagram Protocol (UDP) on the specified port, select **UDP**.

   You can select both if you want to accept both protocol types through the same port.

   In the Symantec AntiVirus example, this would be UDP.
5. Click **OK**.

To add an IP protocol

1. On the Port Control tab, click **New**.



New Port Control

Select:

○ Port number and protocol(s)

● IP protocol

Protocol number: 0

2. In the New Port Control dialog box, to add an IP protocol to the Symantec Client VPN database, select **IP protocol**.
3. In the Protocol number text box, type the number of the IP protocol.

   You can obtain this information from your administrator.
4. Click **OK**.

Deleting a port or IP protocol

If you want to remove the ability for external hosts to send data through a port or IP protocol that you had previously added, you can delete it from the Symantec Client VPN database.

To delete a port or IP protocol

1. In the Symantec Client VPN window, on the Port Control tab, from the Enabled Ports list, select the port or IP protocol that you want to delete.
2. Beside the Enabled Ports list, click **Delete**.

Enabling and disabling file and print sharing

When your computer is connected to a corporate LAN protected by a security gateway, you can use the Enable File/Print Sharing option as a short-cut to enable all the ports that are used by Microsoft networking at one time.

This lets you share your own files or browse the LAN.

For file and print sharing to work, you must also configure the sharing properties for your files and directories using Microsoft Windows.

Caution: Do not enable file and print sharing unless you are protected by another firewall or security gateway.

Table 7-1 Ports and protocols enabled for file and print sharing

Port number	Protocol
cifs (139)	TCP
ndbgram (138)	UDP
netbios_137_tcp (137)	UDP
netbios_137_udp (137)	TCP
netbios_138_tcp (138)	TCP
netbios_139_udp(139)	UDP

Note: You do not need to enable file and print sharing if you already know the names or IP addresses of the file or print shares to which you want to connect

To enable or disable file and print sharing

Because file and print sharing is a security risk on the Internet without another firewall or security gateway present, it is disabled by default.

File and print sharing is immediately enabled or disabled. You do not have to click Apply or restart your system for the changes to take affect.

To enable file and print sharing

1. Verify that you are protected from the Internet by a security gateway.
2. Do one of the following:
   - In the Symantec Client VPN window, on the Port Control tab, check **Enable File/Print Sharing.**
   - In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Enable File and Print Sharing.**

   All ports in the Enabled Ports list are now enabled for file and print sharing.

To disable file and print sharing

◆ Do one of the following:

- In the Symantec Client VPN window, on the Port Control tab, uncheck **Enable File/Print Sharing.**
- In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Disable File and Print Sharing.**

Managing Symantec Client VPN

From the Options tab of Symantec Client VPN, several advanced client features and tools are available to help you manage client connections and fully optimize the client's performance.

Table 8-1 Summary of client management features

Item	Description
Display Log	Lets you view a summary log of the current session's activity, including all notification and process information. See "Viewing log data" on page 106.
System information	Displays information on the operating system, the network adapters and statistics, the current IP routing table, and the tunnel summaries. See "Viewing system information" on page 108.
LiveUpdate	Lets you use Symantec's LiveUpdate feature to check for and update Symantec Client VPN and other Symantec software on your workstation. See "Updating software using LiveUpdate" on page 109.
Delete User	Lets you delete the logged on user. See "Deleting a user" on page 111.

Viewing log data

The Symantec Client VPN log viewer lets you view a detailed description of all messages pertaining to the current session's activity, including all notification and process information.

You can use the log viewer to:

- Detect possible attacks, as indicated by high levels of messages reporting rejected packets.
- Provide information to Symantec's support team when troubleshooting a problem.

The maximum size of the log file size is 2MB. When this size is reached, the current log file is saved in the directory \ OldLogs and a new log file is started in the Symantec Client VPN log viewer. In addition, each time you use Symantec Client VPN, a new log is started.

The default number of log files that is saved is seven. When that number is exceeded, the oldest log file is deleted.

To use the log viewer

Entries in the log are displayed with the most recent activity at the bottom of the window. The following procedures tell you how to:

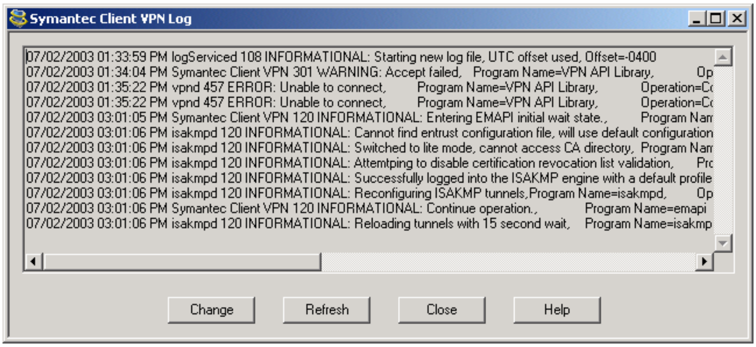
- View log data
- Resize the log file
- Copy data from the log viewer to a file

Note: The log viewer displays a snapshot of the most recent client activity; it does not display real-time data. You can click Refresh to update the view.

To view the log data

1. Do one of the following to display the log viewer:
   - In the Symantec Client VPN window, on the Options tab, click **Display Log.**
   - In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Display Log**.

You can use the icon in the system tray to display the Log viewer even if the Symantec Client VPN dialog box is not open.



```
07/02/2003 01:33:59 PM logServiced 108 INFORMATIONAL: Starting new log file, UTC offset used, Offset=-0400
07/02/2003 01:34:04 PM Symantec Client VPN 301 WARNING: Accept failed,   Program Name=VPN API Library,       Op
07/02/2003 01:35:22 PM vpnd 457 ERROR: Unable to connect,       Program Name=VPN API Library,       Operation=Co
07/02/2003 01:35:22 PM vpnd 457 ERROR: Unable to connect,       Program Name=VPN API Library,       Operation=Co
07/02/2003 03:01:05 PM Symantec Client VPN 120 INFORMATIONAL: Entering EMAPI initial wait state.,      Program Nam
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Cannot find entrust configuration file, will use default configuration
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Switched to lite mode, cannot access CA directory,  Program Nam
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Attemtping to disable certification revocation list validation,     Pro
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Successfully logged into the ISAKMP engine with a default profile
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Reconfiguring ISAKMP tunnels,Program Name=isakmpd,     Op
07/02/2003 03:01:06 PM Symantec Client VPN 120 INFORMATIONAL: Continue operation.,        Program Name=emapi
07/02/2003 03:01:06 PM isakmpd 120 INFORMATIONAL: Reloading tunnels with 15 second wait,   Program Name=isakmp
```

2 Use the following buttons to manage the log data:

Change

Starts a new log file and saves the previous log data in the OldLogs directory.

Two formats are saved:

- A text version, which you can view using a text editor.
  The file name uses the format:
  logfile.txt.<yyyymmdd>
  where yyyy is the year, mm is the month, and dd is the day
- A binary file that can be read using the Symantec gateway security flatten utility.

Refresh

Updates the data in the log viewer.

Close

Closes the log window.

Help

Displays the Symantec Client VPN Online Help system.

3 To close the log viewer, click **Close**.

To resize the log file

1 Move the mouse over an edge of the log viewer until the mouse pointer turns into a double-headed arrow.

2 Drag the window border to resize the window.

You can also maximize or minimize the window using the buttons in the upper right corner.

To copy the data from the log viewer to a file

1. To make sure the log is up to date, click **Refresh**.
2. Right-click on the log text, and then click **Select All**.
3. Right-click again, and then click **Copy**.
   This places the selected data in the Windows paste buffer.
4. Use a text editor (Microsoft Word, Notepad or Word Pad) to open a text file.
5. Paste the copied information into the file.

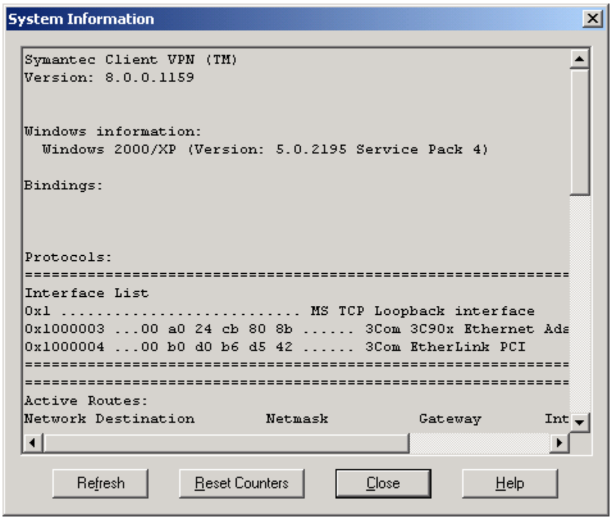
Viewing system information

The System Information dialog box displays information on the operating system, the network adapters, and the current IP routing table. It also provides statistics and tunnel summaries for the current session.

Note: The System Information window displays a snapshot of the most recent client activity; it does not display real-time data. Click Refresh to update the view.

To view the system information

◆ In the Symantec Client VPN window on the Options tab, click **System Information**.



```
Symantec Client VPN (TM)
Version: 8.0.0.1159


Windows information:
  Windows 2000/XP (Version: 5.0.2195 Service Pack 4)

Bindings:



Protocols:
=============================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 a0 24 cb 80 8b ...... 3Com 3C90x Ethernet Ads
0x1000004 ...00 b0 d0 b6 d5 42 ...... 3Com EtherLink PCI
=============================================================
=============================================================
Active Routes:
Network Destination        Netmask           Gateway       Int
```

The following buttons are available to help you manage system information:

Refresh	Updates the snapshot of the data in the window.
Reset Counters	Resets the packet and byte counters to zero in the Symantec Client VPN Information section in the lower part of the display.
Close	Closes the System Information window.
Help	Provides more information on the System Information feature through the Symantec Client VPN Help.

Updating software using LiveUpdate

You can use Symantec's LiveUpdate technology to determine whether there is a more recent version of Symantec Client VPN available and update the Symantec Client VPN software on your workstation to the latest version.

Using your existing Internet connection, LiveUpdate connects to and disconnects from the Symantec LiveUpdate server to check for program and other updates such as virus definitions and URL lists.

When updates are available, you can instruct LiveUpdate to download them to your computer and install them, ensuring that your Symantec software is up-to-date.

If you have any questions or need help while using LiveUpdate, click Help from any LiveUpdate dialog box for further assistance.

To update client software using LiveUpdate

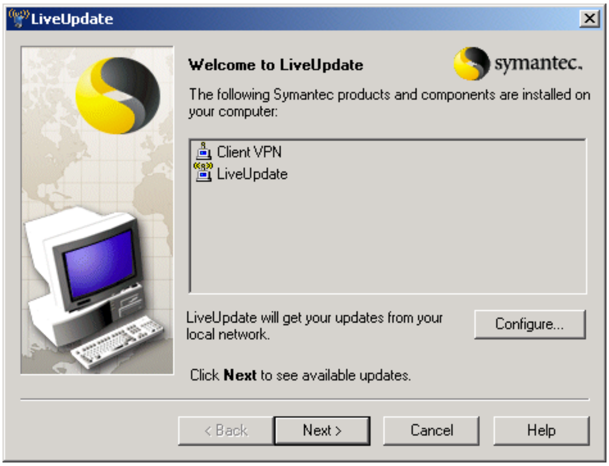
1 Close open applications on your computer.

If LiveUpdate installs products that require a reboot, you will be prompted to restart your computer. You can restart later; however, closing other applications prior to running LiveUpdate allows you to restart immediately.

2 Do one of the following to start LiveUpdate:

- In the Symantec Client VPN window, on the Options tab, click **LiveUpdate**.

- In the Windows system tray, right-click the Symantec Client VPN icon, and then click **LiveUpdate**.



Welcome to LiveUpdate

The following Symantec products and components are installed on your computer:

Client VPN
LiveUpdate

LiveUpdate will get your updates from your local network.

Click **Next** to see available updates.

The Welcome to LiveUpdate dialog box lists the Symantec products that are installed on your computer.

3 Click **Next**.

4 The next LiveUpdate dialog box lists products that are not up to date.

Select the products that you want to update, and then click **Next**.

5 The next LiveUpdate dialog box shows LiveUpdate's progress as it downloads the product updates and installs them.

When the screen indicates that the installations are complete, click **Finish**.

6 If the update requires a reboot, a message is displayed. Do one of the following:

- To reboot now, save any unsaved work in other applications, and then click **Reboot your machine now**.
- To reboot later, click **Continue working in Windows**.

Note: You must reboot before you use the updated applications.

7 Click **OK**.

Deleting a user

When you delete a user, all information that is unique to that user is removed from the Symantec Client VPN database.

Global settings, such as some preferences defined on the Options tab, are not deleted because they apply to all Symantec Client VPN users on this machine.

Table 8-2 User-specific vs. global settings

Type of setting	Settings
User-specific	Security gateways
	Security Gateway groups
	Secure Tunnels
	Time after which inactive tunnels are disconnected
	Whether Save Password is enabled
	Whether Save extended authentication is enabled
	Whether the auto-dial dialog box is displayed on startup
Global	Port control options
	MTU setting
	UDP encapsulation setting
	Minimize on connect setting
	Dynamic source port

To delete users

You can delete a user in two ways:

- From the logon dialog box
  The Delete User option on the logon dialog box lets you delete the user without entering a password.
  This is useful if you want to remove the user but do not know the password.
- From the Options tab
  Deleting the user from the options tab deletes the logged on user.

To delete a user from the Logon dialog box

1. Do one of the following:
   - On the desktop, double-click the Symantec Client VPN icon.
   - In the Windows system tray, right-click the Symantec Client VPN icon, and then click **Open Symantec Client VPN**.
2. In the Symantec Client VPN Logon dialog box, in the User name text box, type the name of the user you want to delete.
3. Click **Delete User**.
4. A screen message warns you that all user information will be deleted and asks if you want to continue.

   Do one of the following:
   - To delete all information for the user, click **Yes**.
   - To return to the Logon dialog box without deleting the user, click **No**.

To delete a logged on user

1. In the Symantec Client VPN window, on the Options tab, click **Delete User**.
2. A screen message warns you that all user information will be deleted and asks if you want to continue.

   Do one of the following:
   - To delete all information for the user, click **Yes**.
   - To return to the Options tab without deleting the user, click **No**.
3. In the Verify password dialog box, type the logon password for the logged on user.
4. To delete the user, click **OK**.

   Symantec Client VPN verifies the password, deletes the logged on user from the client database, and closes the client application.

Section 2

Administering Symantec Client VPN

Use this section of the *Symantec Client VPN User's Guide* if you are an administrator who supports users of Symantec Client VPN.

It contains the following chapters:

- Supporting Symantec Client VPN Users
- Creating installation packages

If you use Symantec Client VPN to connect to protected remote resources, see Section 1, "Using Symantec Client VPN" on page 19 and the appendices.

Chapter 9

Supporting Symantec Client VPN Users

Symantec Client VPN is designed to work with Symantec security gateways in a distributed corporate environment.

Symantec Client VPN can be installed and configured by an individual user who follows the instructions in Section 1 of this book. However, in a complex corporate environment, it is more likely that you, as a Symantec Client VPN administrator, will manage the installation and configuration for your users.

This chapter and the following chapter on the Symantec Packager describe the strategies and tools you need to implement an enterprise-wide deployment of Symantec Client VPN. Such a deployment lets you ensure that the desktop environments of everyone connecting to the corporate network are consistent. That consistency simplifies the roll-out of updates and configuration changes and streamlines troubleshooting procedures.

This chapter includes the following topics:

- Selecting user installation options
- Creating preconfigured or silent installations
- Helping users configure Symantec Client VPN

Selecting user installation options

This section describes installation options that you can provide to users.

The first two options require a minimum of administrative work. You make the full installation kit available to your users either on a CD or through a download site. In both of these scenarios, your users can install by using the standard installation procedure that is described in Chapter 2, "Installing Symantec Client VPN" on page 21.

The other options allow you to customize Symantec Client VPN installation to preset some or all installation choices. The administrative tasks that you perform to do this customization are described in this chapter, and in the following chapter, "Creating installation packages" on page 127.

You can provide users with any of the following installation options:

- Installation from the Symantec Client VPN installation media

  You physically provide the Symantec Client VPN CD to each user.

  To use this method of distribution, make copies of the installation CD up to the number of users for which your corporation is licensed.

  Provide users with any necessary user names or passwords, as described in "Providing required account information to users" on page 122.

- Downloaded installation

  You set up a download site from which your users can download the installation files.

  If you want users to run the CDStart autoinstaller to launch the installation, review documentation, and install Adobe Acrobat, include all the CD contents except the Packager directory.

  If users will install by using setup.exe, the only directory that you need to copy to the download site is AES_3DES_DES.

  Provide users with instructions for accessing the site, and any necessary user names or passwords. as described in "Providing required account information to users" on page 122.

- Preconfigured or silent installation

  Create and distribute a preconfigured installation so that users do not make any installation choices. See "Editing install.inf to create a preconfigured installation" on page 117.

  You can also create a preconfigured installation that is a silent installation by suppressing the installation screens. See "Creating setup.iss to use in silent installations" on page 120.

- Installation packages

  You create and distribute an installation package, which is a single user-executable procedure that installs multiple products to create the remote environment that you want to standardize for your users.

  An installation package can include:

  - Symantec Client VPN installation
  - Other product installations, such as Internet service provider software and extended authentication software
  - Remote policies

    See "About remote policies" on page 124.

  For instructions on creating installation packages, see "Creating installation packages" on page 127.

Creating preconfigured or silent installations

A preconfigured installation lets an end user install without making any installation choices.

You determine how you want Symantec Client VPN installed. Based on those decisions, you create an installation file that runs on the remote systems that will connect users to your corporate network.

You can create a preconfigured installation for Symantec Client VPN in two ways:

- By editing the install.inf file provided with the Symantec Client VPN installation files.

  This creates a preconfigure installation that does not require user input.
- By using the InstallShield silent installation procedure to create a setup.iss file.

  This form of preconfigured installation is silent. In addition to not being required to provide input, the user does not see any installation screens.

Editing install.inf to create a preconfigured installation

You can preconfigure the Symantec Client VPN installation by modifying the file that controls which installation screens are displayed and the default choices for those screens.

To edit install.inf to create a preconfigured installation

1. Copy the Symantec Client VPN installation software to a directory on your system.
2. Navigate to the following directory:
   \ClientVPN\AES_3DES_DES
3. Right-click the file install.inf and select **Properties**.
4. Under Attributes, disable Read-only, and then click **OK**.
5. Double-click install.inf to open it in a text editor of your choice.

   Each installation screen is identified in the file in the following format:

   [*screen*]
   Show=True

   Where *screen* is the name of the InstallShield screen.

   For some screens, there is additional information that represents installation choices.
6. For every screen that you do not want to display during the installation, change the value of the parameter Show= to False.

   For example, to prevent the welcome screen from displaying, make the following change:

Original file	Modified file
[Welcome] Show=True	[Welcome] Show=False

   You can suppress all or some of the installation screens.
7. Preconfigure installation options by changing values in the file.

   You can preconfigure the following:

[Path] Show=True Path=	The Path parameter controls where Symantec Client VPN is installed. The default installation path is: C:\Program Files\Symantec\ClientVPN If you want users to install to a different directory, type the new path as a value for Path=. For example, to install to a directory on the D drive called CorporateVPNClient, you would type: Path=D:\CorporateVPNClient

[Options]
Show=True
AddFolder=True
AddIcon=True
	The Options parameters control the following:
	■ AddFolder
	When the value of this parameter is True, a folder called Symantec Client VPN is added to the user's Program menu.
	To suppress the creation of this folder, change the value to False.
	■ AddIcon
	When the value of this parameter is True, the Symantec Client VPN icon is added to the desktop.
	To suppress the creation of this icon, change the value to False.

[Finish] Show=True	The Finish parameter controls whether the user's computer is restarted at the end of the installation. ■ If the value of Show is True, the final screen of the installation is displayed, allowing the user to restart. ■ If the value of Show is False, the final screen is not displayed and the user's computer is not restarted. If you set Finish to false, instruct your users to restart their computers before they use Symantec Client VPN. If you will use the preconfigured installation in an installation package, you should suppress the restart so that other products can be installed. Configure the installation package to prompt users to perform a single restart. See "Configuring an installation package" on page 136.

8 Save install.inf.

9 Ensure that install.inf is in the same directory as setup.exe when you provide the Symantec Client VPN installation files to your users.

Verifying the preconfigured installation

After you create the preconfigured install, run it to verify that it installs correctly.

To verify the preconfigured installation

1 Ensure that the file install.inf is in the directory that contains the Symantec Client VPN installation software and setup.exe.

2 Run the Symantec Client VPN installation by double-clicking setup.exe.

3 If you did not specify an automatic restart when you created the preconfigured install, restart your computer.

4 Verify that the Symantec Client VPN files are installed to the location that you specified when you modified install.inf.

Creating setup.iss to use in silent installations

You create the file setup.iss by running the Symantec Client VPN installation from the command line with a InstallShield switch that records your installation choices.

When the user runs the installation with the setup.iss file present, no installation screens are displayed.

To create a silent installation using InstallShield

1. Copy the Symantec Client VPN installation software to a directory on your system.
2. Open a DOS window and change directory to the location of the installation software.
3. Run the Symantec Client VPN installation by using the record parameter, as follows:

   setup.exe /r
4. Complete the installation.

   See "Installing Symantec Client VPN" on page 26.

   Use the options that you want to have applied when your users install.

   For example, if you want your users to install to a directory other than the default directory, enter it in the Choose Destination Location dialog box.
5. In the Installation Review dialog box, review the selections you have made and do one of the following:
   - To display previous dialog boxes so that you can change your installation choices, click **Back**.
   - To start the installation, click **Next**.
6. In the InstallShield Wizard Complete dialog box, do one of the following:
   - If you are creating the silent installation for use in an installation package, click **No, I will restart my computer later**.

     This lets you add other products to the package, so that the user only has to restart once after all products have installed.

     See "Creating installation packages" on page 127.
   - If you are creating the silent installation to be used stand-alone, click **Yes, I want to restart my computer now**.

     If you choose to restart the computer when you create the silent installation, a restart will be performed automatically when the user installs.

7 Click **Finish**.

8 If you did not specify an automatic restart in step 6, restart your system.

Verifying the silent installation

After you create the silent installation, run it to verify that it installs correctly.

To verify the silent installation

1 Uninstall Symantec Client VPN.
See "Uninstalling Symantec Client VPN" on page 31.

2 Locate the setup.iss file.
This will be in the WINNT directory if you are running Windows 2000 or Windows NT.
It will be in the Windows directory if you are running Windows XP.

3 Copy setup.iss to the directory that contains the Symantec Client VPN installation software.

4 Run the Symantec Client VPN installation by using the silent mode parameter, as follows:
setup.exe /s

5 If you did not specify an automatic restart when you created the silent install, restart your computer.

6 Verify that the Symantec\ClientVPN directory is created in the location that you specified when you created the silent install.
By default, this is C:\Program Files\Symantec\ClientVPN

Deploying preconfigured and silent installations

After you create a preconfigured or silent installation, you can use it in an installation package. See "Creating installation packages" on page 127.

You can also deploy these installations directly to your users if there is no other software that you want them to install in conjunction with Symantec Client VPN.

To deploy a preconfigured or silent installation

1 Copy the Symantec Client VPN installation files to a download server.

2 In the \ClientVPN\AES_3DES_DES directory, include the file that runs the silent installation.
Depending on how you created the installation, this can be either install.inf or setup.iss.

3. Provide users with instructions for accessing the site, any necessary user names or passwords, and instructions for running the silent installation.

   For example, if you have suppressed the restart at the end of the installation, you should tell users that they have to restart their machines before they can use Symantec Client VPN.

Helping users configure Symantec Client VPN

Symantec Client VPN must be configured before a user can connect to the corporate network.

As the Symantec Client VPN administrator, you have several options to assist users with configuration:

- Configure the client desktops yourself, or with the help of a team of IT administrators.

  In this case, you will complete the configuration procedures that are described in:

  - Chapter 4, "Configuring security gateways" on page 49
  - Chapter 5, "Configuring and connecting security gateway groups" on page 79

- Provide users with the configuration information that is required for connection, so that they can perform the configurations themselves.

  See "Providing required account information to users" on page 122.

- Provide users with remote policies.

  See "About remote policies" on page 124.

Providing required account information to users

For each user, verify that an account has been established and that security gateways have been properly configured.

Obtain one of the following for your users:

- Remote policies that contain the users' security gateway configurations

  See "About remote policies" on page 124.

- Configuration information that you or your users will need to configure the security gateways

If you or your users will configure security gateways, obtain the following information from the security gateway administrator:

- The IP address or fully qualified domain name of the security gateway to which the user will connect.
- The user's Client Phase 1 ID.
- The user's Gateway Phase 1 ID (if applicable and if it differs from the security gateway IP address).
- One of the following:
  - If the user will authenticate using a shared secret, the shared secret that is defined on the security gateway.
  - If the user will authenticate using a digital certificate, from the security gateway administrator, obtain a profile with the certificate (for example, user.epf) and the user's certificate password.
- If your network uses a form of extended authentication (for example, a Defender Server or a SecurID ACE/Server), provide the user with all of the necessary cards, tokens, user names, and passwords for the specified method.
- If the security gateway administrator has created a remote policy for use in configuring Symantec Client VPN, provide the user with the remote policy file and a remote policy install password.

  See "About remote policies" on page 124.

In addition, if the security gateway to which your users will connect does not support autodownload of VPN policies and tunnel information, obtain the following:

- IKE policy details for each security gateway
- IP address and subnet mask for each secure tunnel
- VPN policy details for each secure tunnel

About remote policies

Remote policies are created by your security gateway administrator. They contain the configuration information necessary to establish a secure tunnel from the system running Symantec Client VPN to the corporate network.

Appendix A, "Remote policies" on page 141, describes remote policies from the end user point of view.

Administrators can create two kinds of remote policies:

- Individual remote policies for each remote user
- A single remote policy that can be used to configure all remote systems

  The use of a single remote policy is possible if your organization uses an extended authentication method such as Defender, LDAP, or SecurID ACE/ Server to authenticate VPN users. When extended authentication is used, the administrator can define a single default-ikeuser on the security gateway.

  The administrator then creates a remote policy for the default-ikeuser. This remote policy allows Symantec Client VPN users with any client Phase 1 ID to authenticate.

  To distribute a remote policy to all users as part of an installation package, you would use a remote policy for default-ikeuser.

Distributing remote policies to your users

As the Symantec Client VPN administrator, you provide the remote policy files to your users and ensure that they understand how to use them.

The security gateway administrator will provide you with a zip file that contains one or more remote policies.

To distribute remote policies to users

1. Create a deployment directory.
2. Copy the remote policy zip file to the directory.
3. Unzip the remote policy file so that you have individual files.

   The files are named as follows:

   <username>.rm7

   where <username> is the name of the user.

4. Prepare instructions for your users on how to install the remote policies.

   The instructions will depend on how the Symantec Client VPN software will be installed:

   - If the user will install Symantec Client VPN directly, or by using a silent installation, instruct the user to copy the remote policy file to the directory that contains setup.exe.

     The remote policy is installed to the \ClientVPN directory when Symantec Client VPN is installed.
   - If you are providing an installation package and receive a remote policy, you can include it in the package.

     See "Creating installation packages" on page 127.

     When the installation package is run on the client machine, the remote policy is installed to the \ClientVPN directory.
   - If you receive remote policies after your users have installed Symantec Client VPN, instruct them to copy the remote policy to the \ClientVPN directory.
5. Distribute the remote policy files to your users, along with the instructions on how to install them.

Chapter 10

Creating installation packages

This chapter provides a high level description of Symantec Packager, which is provided on your *Symantec Client VPN* CD for use in building an installation package containing Symantec Client VPN.

Symantec Packager lets you create, modify, and build custom installation packages that you distribute to target systems. Using Symantec Packager, you can tailor installations to fit your corporate environment, building packages that contain only the features and settings that your users need.

Symantec products included in installation packages are protected by copyright law and the Symantec license agreement. Distribution of packages requires a license for each user who installs the package.

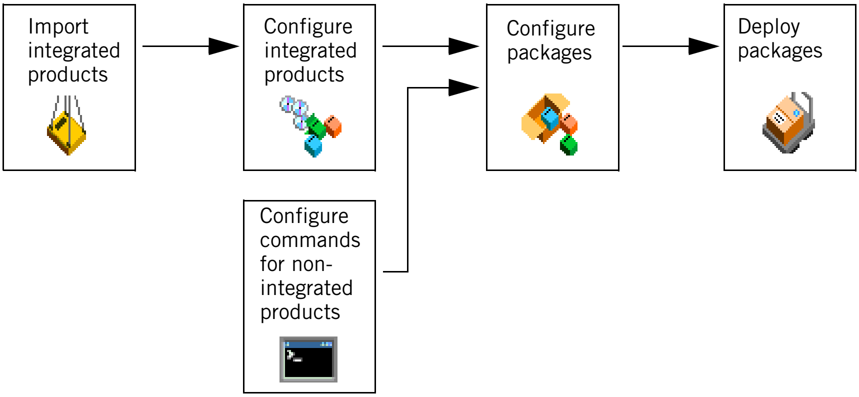
Your users can install installation packages created with Symantec Packager on all Microsoft 32-bit platforms except for Windows NT 3.51.

This chapter includes the following topics:

How Symantec Packager works

How you create the installation package depends on whether the software you want to include is integrated with Symantec Packager or not.

Figure 10-1 Overview of Symantec Packager phases


Import integrated products
Configure integrated products
Configure packages
Deploy packages
Configure commands for non-integrated products

The process of creating the installation package involves the following:

- Adding product installations by:
  - Importing integrated products and configuring them using the Product Editor.

    You include integrated software such as pcAnywhere by importing the product module of the integrated product. The product module contains installation binary files and template files that let you control how the product is installed.
  - Creating custom installation commands for Symantec Client VPN and any other product that is not integrated.

    You include non-integrated products such as Symantec Client VPN in the installation package by configuring commands.

  See "Adding products to an installation package" on page 132.
- Configuring an installation package that contains all of the products you want the user to install.

  See "Configuring an installation package" on page 136.
- Deploying the installation package.

  See "Deploying an installation package" on page 139.

Installing Symantec Packager

The Symantec Packager software runs on Windows NT, Windows 2000, and Windows XP Professional platforms only.

The Symantec Packager software and documentation are included on the *Symantec Client VPN* CD in the following locations:

\Packager\Kit	Symantec Packager installation files
\Packager\Documentation	*Symantec Packager Implementation Guide*

Before you begin, you should read the *Symantec Packager Implementation Guide* for detailed system requirements and installation instructions.

To install Symantec Packager

1. Insert the *Symantec Client VPN* CD in the CD-ROM drive.
2. Navigate to the \Packager\Kit directory.
3. Double-click setup.exe.
4. Complete the installation as described in the *Symantec Packager Implementation Guide.*
   You are not required to restart your system.

Planning an installation package

Planning how you will create an installation package, includes the following:

- Identifying the products for the package
- Determining the level of user interaction during installation

Identifying the products for the package

Before you create an installation package, determine whether the products you want to include with Symantec Client VPN are integrated with the Symantec Packager. Whether products are integrated or not affects how you include them in the installation package.

The Symantec Packager lets you wrap integrated Symantec products, Symantec products that are not integrated, and third-party products into one install.

You can include any of the following:

- Symantec Client VPN
- A remote policy
  See "About remote policies" on page 124.
- An extended authentication method
- Virus protection software
- Internet connection software

Preparing to customize integrated products

For integrated products, you can do all your customization within Symantec Packager. The following products are integrated with Symantec Packager:

- Symantec AntiVirus Corporate Edition, Server and Client
- pcAnywhere
- Symantec Client Firewall

Before you begin to create the installation package, for each product, determine the product features and configuration files that you want to have installed on user computers, and plan the installation options that will be used.

Creating silent installs for non-integrated products

For each product that is not integrated, which includes Symantec Client VPN, before you create an installation package, you may want to create a preconfigured or silent installation. If you want the installation package to run without interruptions, make sure that these installations do not require restarts.

Note: The last product that will be installed when the installation package is run can include a restart.

To create silent installs for non-integrated products

1. For Symantec Client VPN, follow either of these procedures:
   - “Editing install.inf to create a preconfigured installation” on page 117
   - “Creating setup.iss to use in silent installations” on page 120
2. Other products that you will include may or may not support silent install functionality. Refer to their supporting documentation to determine the level of support for silent installs and how to configure them to install in this manner.

   For products that support the use of setup.iss, follow the procedure in “Creating setup.iss to use in silent installations” on page 120.

   The documented procedure is specific to Symantec Client VPN; however, the general steps of the procedure can be used to create a silent installation for any software product that installs using InstallShield.
3. For each product, test the silent installation as described in “Verifying the silent installation” on page 121.

Determining the level of user interaction during installation

Symantec Packager lets you specify the level of user interaction required during installation. You can create any of the following:

- A silent installation

  You configure the installations for all products included in a silent installation package so that the user does not have to make any installation choices or see any installation screens.

  For products that are not integrated with Symantec Packager, you must create silent installations for each product prior to including the products in the installation package.

  For products that are integrated with Symantec Packager, you can use Symantec Packager to configure the product installation.
- A passive installation

  Only status information is displayed: the products that are installed are preconfigured.
- An interactive installation

  The package installation includes installation screens that require user interaction.

The procedures in this chapter describe how to create a silent package installation. For instructions on creating a passive or interactive installation, see the *Symantec Packager Implementation Guide*.

Adding products to an installation package

Use Symantec Packager to include multiple products in a single installation package.

To add products to an installation package

There are two procedures for adding products to an installation process:

- Importing an integrated product

  The procedure for importing an integrated product is an overview.

  For more detailed information, see the *Symantec Packager Implementation Guide* and the documentation for the products that you want to include in the installation package.

- Including Symantec Client VPN and other non-integrated products

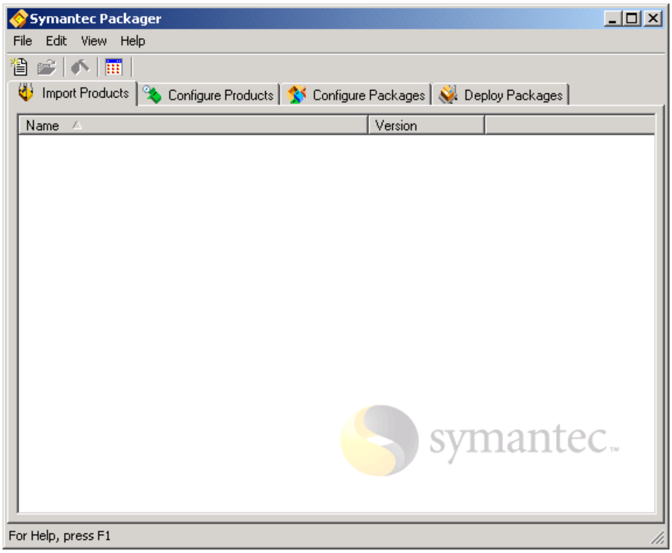
  This topic provides a detailed procedure for using a custom command to include Symantec Client VPN in an installation package.

  You can use the same procedure to include any other product that is not integrated with Symantec Packager.

You should test each product installation that you add before you configure the installation package.

To import an integrated product into an installation package

1 On the Windows taskbar, click **Start** > **Program Files** > **Symantec Packager.**



2 On the Import Products tab, on the File menu, click **Import New Product**.

3 In the Open dialog box, navigate to the folder that contains the product module that you want to import.

4 Select the product module, and then click **Open**.

Symantec Packager imports the product module and returns you to the Import Products tab.

5 To customize the product installation, see the section on configuring custom products in the *Symantec Packager Implementation Guide*.

To include Symantec Client VPN in an installation package

1 Copy the Symantec Client VPN installation files to a directory on the computer that is running Symantec Packager.

Ensure that all the Symantec Client VPN files that you want to include are in this directory. These can include:

- The install.inf file you created for a preconfigured installation or the setup.iss file you created for a silent installation

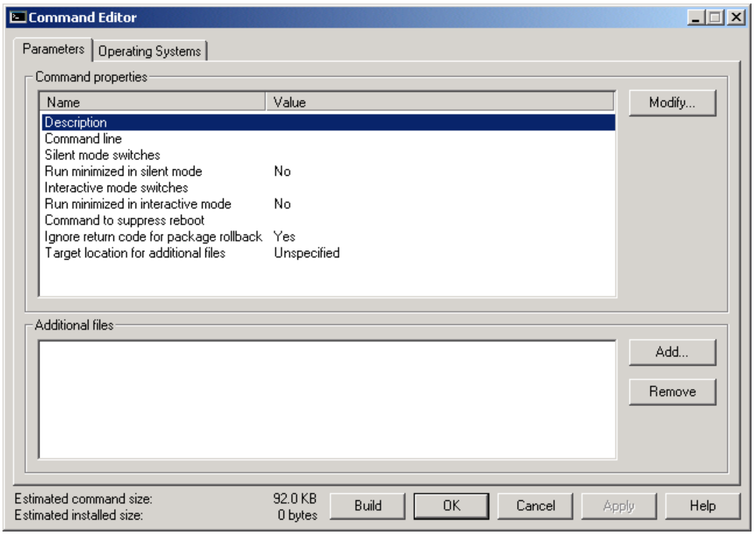
  See "Editing install.inf to create a preconfigured installation" on page 117 and "Creating setup.iss to use in silent installations" on page 120.

- An enterprise-wide remote policy file provided by the security gateway administrator

  Remote policies contain the configuration information necessary to establish a secure tunnel from the system running Symantec Client VPN to the corporate network.

  See "About remote policies" on page 124.

2 In the Symantec Packager window, on the Configure Products tab, on the File menu, click **New Custom Command**.



Name	Value
Description	
Command line	
Silent mode switches	
Run minimized in silent mode	No
Interactive mode switches	
Run minimized in interactive mode	No
Command to suppress reboot	
Ignore return code for package rollback	Yes
Target location for additional files	Unspecified

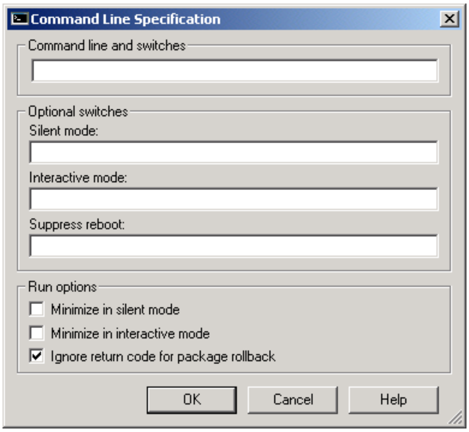
Estimated command size: 92.0 KB
Estimated installed size: 0 bytes

3 In the Command Editor dialog box, on the Parameters tab, select **Description**, and then click **Modify**.

4 In the Command Description dialog box, type a description for the command, and then click **OK**.

Make sure the description is clear enough to help you identify the configuration when you want to use it in an installation package.

5 On the Parameters tab, select **Command line**, and then click **Modify**.



☐ Minimize in silent mode
☐ Minimize in interactive mode
☑ Ignore return code for package rollback

6. In the Command Line Specification dialog box, under Command line and switches, type the Symantec Client VPN executable setup.exe and any switches that are needed to run it.

   - If this command is for a silent installation that uses the setup.iss file, add the /s switch, as follows:

     setup.exe /s

   - If this command is for a preconfigured installation of Symantec Client VPN that uses a modified install.inf file and you suppressed the Finish screen as part of the modification, you do not need to specify a switch.

     If you did not suppress the Finish screen when you modified install.inf, enter the setup command with the noreboot switch, as follows:

     setup.exe /NOREBOOT

7. Click **OK**.

8. On the Parameters tab, beside the Additional Files list, click **Add**.

9. In the Open dialog box, browse to the location of the Symantec Client VPN installation files.

10. Select all the files, and then click **Open**.

    The files are added to the Additional Files list.

11. On the Parameters tab, click **Build**.

12. In the Save As dialog box, type a name for the configuration file, and then click **Save**.

    The Command Build Status dialog box shows the progress of the build.

13. When the line "Command was built successfully" is displayed, click **Close**.

To test the installation of configuration files

1. Open Windows Explorer and browse to the working directory that is displayed in the Symantec Packager window on the Configure Products tab.

   If you are running Microsoft Windows 2000 or Windows XP and have not changed your Symantec Packager preferences, this will be:

   C:\Documents and Settings\<user>\My Documents\Packager

   Where <user> is the logon name of the user who installed Symantec Packager.

   If you are running Windows NT 4.0, this will be:

   C:\Winnt\Profiles\<user>\My Documents\Packager

2. Expand the Deployment folder to see your configuration files.

   Each file is a self-extracting executable file.

3 To launch the installation, double-click the file that you want to test.

4 When the installation completes, test the installed product to ensure that it functions correctly.

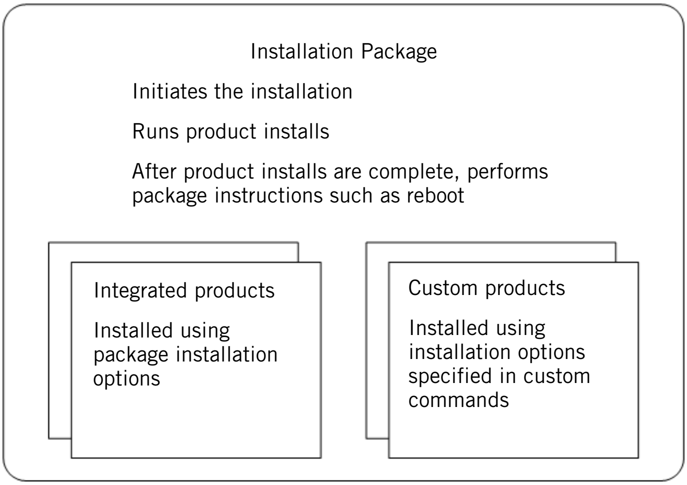
Configuring an installation package

To configure an installation package, add the product configurations and custom commands that you created using the Configure products tab to a package. You can further customize the package by setting package installation options, product installation order, and other settings.

When you build the package, Symantec Packager creates an installation file that incorporates the product, command, and package options that you specified.

The installation package acts as a wrapper around the products that are included in it. The package initiates the installation and runs the integrated product installations and custom commands.

Figure 10-2 Installation package


Installation Package
Initiates the installation
Runs product installs
After product installs are complete, performs package instructions such as reboot
Integrated products
Installed using package installation options
Custom products
Installed using installation options specified in custom commands

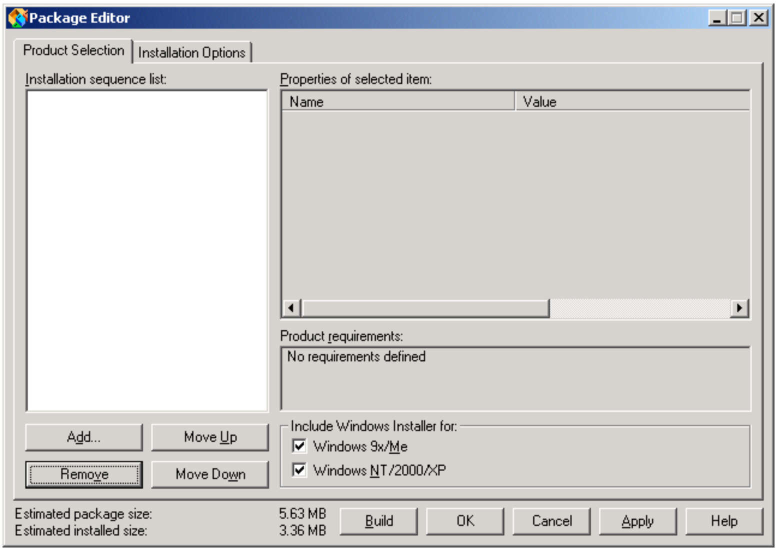
How individual products within the package are installed depends on whether they are integrated with Symantec Packager or not. Integrated products adhere to the installation choices you make for the package, while custom products are installed based solely on what you specify in the custom command.

When all the products in the package have been installed, the package installer determines whether a reboot is necessary and initiates it if required.

The following procedure summarizes the tasks you can do on the Configuration tab. For more information, see the *Symantec Packager Implementation Guide*.

To configure an installation package

1. In the Symantec Packager window, on the Configure Packages tab, on the File menu, click **New Package Definition**.



No requirements defined

☑ Windows 9x/Me
☑ Windows NT/2000/XP

Estimated package size: 5.63 MB
Estimated installed size: 3.36 MB

2. In the Package Editor dialog box, under Installation Sequence list, click **Add**.

3. In the Open dialog box, from the list of files in the Packages directory, select the .pcg file for a product that you want to add to the installation package, and then click **Open**.

4. Repeat steps 2 and 3 for each product you want to include in the package.

5. To determine the order in which the products will be installed, reorder the Installation sequence list as follows:

   - Select a product in the list.
   - Click **Move Up** or **Move Down**.

   If a product's preconfigured installation includes a restart, make it the last product in the package.

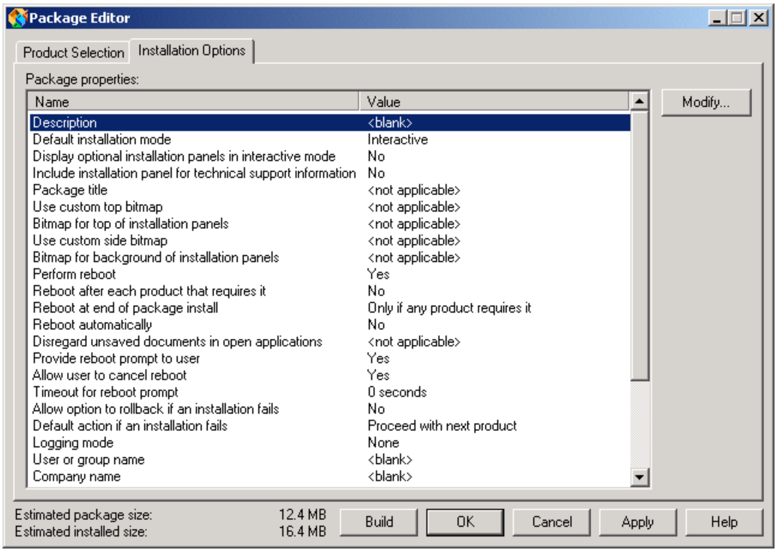
6. Under Include Windows Installer for, determine whether you need to include Windows installer in your installation package.

   If users will install Symantec Client VPN by itself, Windows Installer is not required.

If Symantec Client VPN is included in a package generated by the Symantec Packager, Windows Installer version 2.0 is required.

- If Windows Installer is already on the target machines to which this package will be installed, you can uncheck the options.
- If you do not know whether Windows Installer is available, leave these options checked.

7 On the Installation Options tab, select Description, and then click **Modify**.



Package properties:

Name	Value
Description	<blank>
Default installation mode	Interactive
Display optional installation panels in interactive mode	No
Include installation panel for technical support information	No
Package title	<not applicable>
Use custom top bitmap	<not applicable>
Bitmap for top of installation panels	<not applicable>
Use custom side bitmap	<not applicable>
Bitmap for background of installation panels	<not applicable>
Perform reboot	Yes
Reboot after each product that requires it	No
Reboot at end of package install	Only if any product requires it
Reboot automatically	No
Disregard unsaved documents in open applications	<not applicable>
Provide reboot prompt to user	Yes
Allow user to cancel reboot	Yes
Timeout for reboot prompt	0 seconds
Allow option to rollback if an installation fails	No
Default action if an installation fails	Proceed with next product
Logging mode	None
User or group name	<blank>
Company name	<blank>

Estimated package size: 12.4 MB
Estimated installed size: 16.4 MB

8 In the Package Description dialog box, type a description for the installation package, and then click **OK**.

9 Select Default installation mode, and then click **Modify**.

10 In the Default installation mode dialog box, specify the level of user interaction required during installation, and then click **OK**.

Note: If your package includes products that are integrated with Symantec Packager, be aware that the type of interaction you choose here should correspond with the type of interaction you specified when configuring the integrated products.

11 Symantec Client VPN installation requires a restart. If you suppressed restarts in the silent installs of the products in the installation package, you must set restart options for the package so that at the end of the package installation a restart is performed.

To set restart options, complete the following steps:

- Select Perform reboots, and then click **Modify**.
- In the Reboot options dialog box, select **Delay reboot until end of package installation**.
- Uncheck **Only reboot if a product requires it**.

You can also set other options using the Reboot options dialog box. For more information, see the *Symantec Packager Implementation Guide*.

12 To modify any other installation option, select it, and then click **Modify**.

The additional dialog boxes are described in the *Symantec Packager Implementation Guide*.

13 Click **Build**.

The Package Build Status dialog shows the progress as the package builder builds the products you have included into a single, self-extracting .exe file.

14 When the build is complete, to close the Package Builder Status dialog box, click **Close**.

15 To close the Package Editor, click **OK**.

Deploying an installation package

Installation package deployment defines the method by which the installation of a package that contains Symantec Client VPN is launched on your users' remote computers.

During the Deploy Packages phase, you select one or more installation packages for deployment using the Package Deployment tool, which is a Web-based Deployment tool. If you do not want to use the Package Deployment tool, you can use a third-party deployment tool such as Microsoft Systems Management Server, or you can send the installation package to your users and instruct them to run it on their computers.

The *Symantec Packager Implementation Guide* describes the requirements for deploying packages using the Package Deployment tool. If you will use another deployment tool, for requirements, see the documentation for that tool.

You have several options for deploying an installation package:

- Install the package on the local machine, which is the computer that is running Symantec Packager.

  You can use this option to test how the package will install when you deploy it to your organization.

- Deploy the installation package to one or more target machines in your network, using the Package Deployment tool that is part of Symantec Packager.
- Copy deployable files for use with another deployment tool.

  The packages listed on the Deployment tab are self-extracting executable (.exe) files that can be deployed through other deployment tools that support deploying .exe files.

Appendix A

Remote policies

If you will connect to a Symantec security gateway, your administrator can create a remote policy for you that contains pre-defined VPN settings. You receive the remote policy as a file that is named <username>.rm7 where <username> is your user name.

The use of a remote policy simplifies the amount of configuration that you must perform. You do not need to enter this basic configuration information using the Symantec Client VPN user interface.

This appendix includes the following topics:

Information included in a remote policy

The following information may be included in each remote policy file:

- IP address or fully qualified domain name of the security gateway
- Authentication method that Symantec Client VPN must use

  This method is either “shared secret” or “certificate.”

  - If the authentication method is shared secret, the shared secret value is included.
  - If the authentication method is certificate, your administrator will provide you with a certificate file.
- Client Phase 1 ID

  This is the user name with which you will authenticate.
- Gateway Phase 1 ID

  If a Phase 1 ID other than the security gateway’s IP address is defined, a Gateway Phase 1 ID is included.

How Symantec Client VPN processes remote policies

When Symantec Client VPN starts, the software detects the remote policy and processes it as follows:

- The software opens each remote policy that has been copied to the directory where Symantec Client VPN is installed and ensures that it is compatible with the Symantec Client VPN version.
- For each security gateway entry it finds in the remote policy, Symantec Client VPN updates the <username>.dat file. If there is already a security gateway definition for a given IP address in the configuration files, the software overwrites it.
- If a security gateway record uses a certificate as an authentication method, the software displays a message box that tells you to get a certificate from the administrator and configure the certificate before connecting to the security gateway.
- When the software loads a policy, it logs the action to the client log file, as well as any errors that occur.

Symantec Client VPN processes remote policies where the Phase 1 ID is default-ikeuser by using dynamic authentication, as follows:

- The software prompts you for the user ID for the external authentication server, and uses this value as the Phase 1 ID for that security gateway connection.
- If you do not type an ID, the application generates a Phase 1 ID based on the time of the policy. This ensures that all Phase 1 IDs are unique for each security gateway.

Installing remote policy files

You must make sure that you copy your remote policy files to the correct place so that they are loaded when you run Symantec Client VPN.

You have two options:

- If you downloaded your Symantec Client VPN installation files, before you install, copy the remote policy file to the location of the setup.exe file that launches the Symantec Client VPN installation.

  This lets the installation process install the remote policy when the Symantec Client VPN software is installed.
- If you receive a remote policy file after you have installed Symantec Client VPN, or if you install Symantec Client VPN from a CD-ROM, copy the remote policy file to the ClientVPN directory.

  If you install to the default location, this is:

  C:\Program Files\Symantec\ClientVPN

You may receive multiple remote policies in a zip file. If you do, unzip the file and then copy the remote policies to the correct location.

Using remote policies

If there is a remote policy in the ClientVPN directory, Symantec Client VPN processes it automatically when it starts.

You can use the connections that are defined by the remote policy immediately, and continue to use them each time you run Symantec Client VPN.

To use a remote policy

1 Log on to Symantec Client VPN, as described in "Logging on to Symantec Client VPN" on page 34.

  When the log on finishes, you are prompted to load the remote policy:

  Remote Policy Bundle found. Load Bundle <username>.rm7.

  where <username> is your user name.

2 Click **Yes**.

  If a password is required, a dialog box prompts you for the remote policy install password.

3 Type the password that your system administrator has provided.

4 In the Symantec Client VPN dialog box, on the Gateways tab, the connections that are defined by the remote policy appears in the Security Gateways list. To use one of the predefined security gateways, select it, and then click **Connect**.

After Symantec Client VPN processes a remote policy, it moves the remote policy file to the C:\Program Files\Symantec\ClientVPN\oldpolicies folder.

Using multiple remote policies

It is possible to have multiple remote policies on your client workstation. For example, if you need to connect to two different security gateways, your system administrator can generate a remote policy for you on each security gateway.

If you receive multiple remote policies in a zip file, unzip the file and then copy the remote policies to the correct location.

If you copy multiple remote policies to the ClientVPN directory, when you start Symantec Client VPN you are prompted for each policy in turn. If you accept the policies, the security gateway information for each policy is listed on the Symantec Client VPN dialog box Gateways tab.

Restoring old remote policies

After Symantec Client VPN processes a remote policy, it moves the remote policy file to the C:\Program Files\Symantec\ClientVPN\oldpolicies folder. You can restore the security gateway information provided in an old remote policy.

To restore an old remote policy

1. Log off from Symantec Client VPN.
2. Move the required remote policy file from the oldpolicies directory to the ClientVPN directory.
3. Log on to Symantec Client VPN.

   You are prompted to accept the remote policy.

Appendix B

Using digital certificates

A digital certificate lets Symantec Client VPN authenticate without defining a shared secret.

The administrator creates the Entrust certificate profile and provides it to you. When you place this file in the ClientVPN directory and configure it, it authenticates you when you log on to Symantec Client VPN.

This appendix includes the following topics:

- Configuring Symantec Client VPN to use a digital certificate
- Using a digital certificate
- Restoring default digital certificates

Configuring Symantec Client VPN to use a digital certificate

Before you can use a digital certificate to log on, you must configure Symantec Client VPN to use it. To perform the configuration, you must have:

- A profile containing the certificate
- A password to decrypt your private key in the profile
- The Gateway Phase 1 ID required by the security gateways

If you know that you will be connecting using certificate authentication but have not received this information, contact your system administrator.

To configure a digital certificate

1 Using Windows Explorer, copy the profile that contains the certificate to the directory where the Symantec Client VPN software is installed.

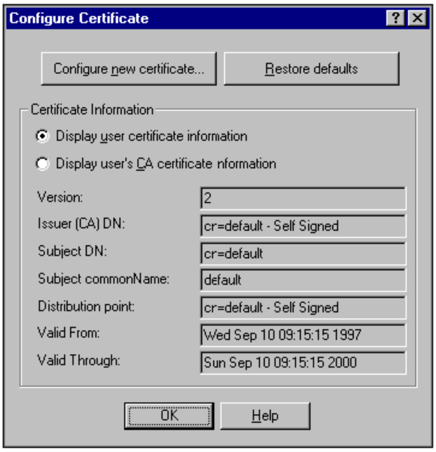
This file has the naming format <user>.epf, where <user> is your user name.

For example, if you installed to the default directory, copy the profile to:

C:\Program Files\Symantec\ClientVPN

2 Log on to Symantec Client VPN.

3 In the Symantec Client VPN dialog box, on the Options tab, click **Configure Certificate.**



Certificate Information

● Display user certificate information

○ Display user's CA certificate nformation

Version:	2
Issuer (CA) DN:	cr=default - Self Signed
Subject DN:	cr=default
Subject commonName:	default
Distribution point:	cr=default - Self Signed
Valid From:	Wed Sep 10 09:15:15 1997
Valid Through:	Sun Sep 10 09:15:15 2000

4 In the Configure Certificate dialog box, click **Configure new certificate.**

5 In the Entrust Profile dialog box, type the name of your Entrust profile file, and then click **OK**.

6 In the Entrust Password dialog box, type your Entrust password, and then click **OK**.

7 At the message indicating that the certificate has been configured, click **OK.**

8 Click **Log Off**.

9 Using a text editor, edit the config.cf file in the directory that contains the Symantec Client VPN installation files, by default ClientVPN.

10 Uncomment the following line:

```
isakmpd.enforce_id_in_cert=0
```

11 Log back in on Symantec Client VPN.

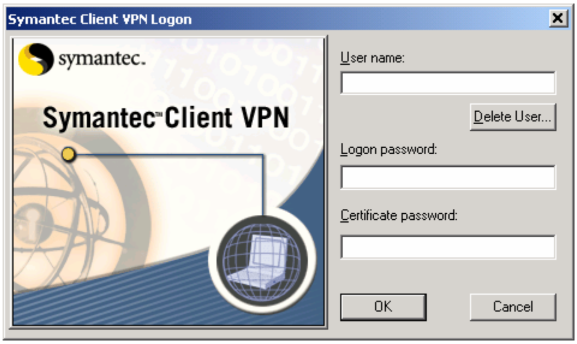
Using a digital certificate

After you have configured your certificate, you invoke it as part of your log on to Symantec Client VPN by providing the certificate password.

To use a certificate

1 Do one of the following:

- On the desktop, double-click Symantec Client VPN.
- In the Windows system tray, right-click the Symantec Client VPN icon and select **Open Symantec Client VPN**.
- Select **Start** > **Program Files** > **Symantec Client VPN** > **Symantec Client VPN**.



2 In the Symantec Client VPN Logon dialog box, do the following:

- In the User name text box, type a name.
- In the Logon password text box, type a password.
- In the Certificate password text box, type your certificate password.
- Click **OK**.

For more information about the logon procedure, see "Logging on to Symantec Client VPN" on page 34.

Restoring default digital certificates

A digital certificate lets Symantec Client VPN authenticate without defining a pre-shared secret.

Once you have configured and logged on using a new digital certificate, you may want to restore the defaults for the Entrust digital certificate on your system.

To restore the default digital certificate

1 In the Symantec Client VPN dialog box, on the Options tab, click **Configure Certificate**.

2 In the Configure Certificate dialog box, click **Restore defaults**.
A message box informs you if the certificate is properly configured.
The values in the Certificate Information section show the restored defaults:

Field	Description
Version	The version of the X.509 standard that applies to the certificate
Issuer (CA) DN	The X.500 name of the authority that signed the certificate
Subject DN	The distinguished name of the user whose public key the certificate identifies
Subject commonName	The user's common name
Distribution point	An ID for Certificate Revocation List (CRL) requests
Valid From	The date and time the certificate is first valid
Valid Through	The date and time the certificate expires

3 Click **OK**.

Appendix C

Troubleshooting

You can find up-to-date troubleshooting information for Symantec Client VPN (and all Symantec products) on the Symantec Web site, www.symantec.com.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access Symantec Client VPN troubleshooting information

1. Go to www.symantec.com/techsupp/enterprise/select_product_kb.html.
2. Under select a knowledge base, scroll down, and then click **Symantec Client VPN**.
3. Click on your specific product name and version.
4. On the knowledge base page for Symantec Client VPN, do any of the following:
   - On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
   - On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed, and then click **Search**.
   - On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Appendix D

Licensing

This appendix describes the licensing requirements for Symantec Client VPN.

User licensing for Symantec Client VPN

The Symantec Client VPN software is licensed with the associated appliance and/or software product. The Symantec Client VPN software version must match the associated appliance software version and/or software version.

The licensing for Client-to-Gateway VPN is by the number of concurrent VPN sessions. For example, you may have 100 users who need VPN access as part of their normal work habits, but at any time, only 10 users are ever connected by way of the VPN. In this situation, you only need a license for 10 concurrent VPN sessions. The appliance and/or software product counts the number of concurrent Client-to-Gateway VPN sessions and stops creating new sessions when the limit is reached.

You are licensed to load the Symantec Client VPN software on as many nodes as you like, but these clients are licensed for use only with the accompanying appliance and/or software product.

Additive user licenses

Additive user licenses are available for Client-to-Gateway VPN. Client-to-Gateway VPN user licenses are independent of node licenses and the two can have different values.

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network

D. use the Software in accordance with any written agreement between You and Symantec; and

E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor

G. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export or re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of the Software to any entity not authorized by, or that is specified by, the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA

Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Index